NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER-ENABLED UNCONVENTIONAL WARFARE: THE CONVERGENCE OF CYBERSPACE, SOCIAL MOBILIZATION, AND SPECIAL WARFARE

by

Ryan S. Gladding
Sean P. McQuade

December 2015

Thesis Advisor: Hy Rothstein
Second Reader: Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE CYBER-ENABLED UNCONVENTIONAL WARFARE: THE CONVERGENCE OF CYBERSPACE, SOCIAL MOBILIZATION, AND SPECIAL WARFARE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Ryan S. Gladding and Sean P. McQuade	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The United States currently faces an environment of constrained resources and increasing threats where new foreign policy options need to be considered. An area that holds the potential for low-profile campaigns to confront enemies of the United States is cyber-enabled unconventional warfare (UW). Conducting military operations through cyber-enabled UW is less expensive, and inherently, it involves less physical risk than a conventional deployment of U.S. military personnel abroad. This research indicates that seven conditions exist in the cyberspace environment that can enhance the conduct of UW. Since no organization in the U.S. military with the requisite capabilities to exploit these conditions in the cyber domain exists, one should be created. Cyber-enabled UW can provide scalable military options to U.S. policymakers that are currently not available.

14. SUBJECT TERMS attack, collective action, computer networks, conflict, cyber-attacks, cyber militia, cyber operations, cyber space, cyber warfare, cyber terrorism, DDoS attacks, department of defense, hackers, hacktivists, hybrid warfare, information warfare, insurgency, Internet, irregular warfare, military capabilities, military doctrine, military strategy, non-state actors, social movement theory, social network analysis, special forces, special operations command, special operations forces, strategic implications, technology, troll army, unconventional warfare, warfare	**15. NUMBER OF PAGES** 117
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89) Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CYBER-ENABLED UNCONVENTIONAL WARFARE: THE CONVERGENCE OF CYBERSPACE, SOCIAL MOBILIZATION, AND SPECIAL WARFARE

Ryan S. Gladding
Major, United States Army
B.A., University of Nevada, Las Vegas, 2003

Sean P. McQuade
Major, United States Army
B.S., Northeastern University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS
AND
MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

NAVAL POSTGRADUATE SCHOOL
December 2015

Approved by: Hy Rothstein
Thesis Advisor

Dorothy Denning
Second Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States currently faces an environment of constrained resources and increasing threats where new foreign policy options need to be considered. An area that holds the potential for low-profile campaigns to confront enemies of the United States is cyber-enabled unconventional warfare (UW). Conducting military operations through cyber-enabled UW is less expensive, and inherently, it involves less physical risk than a conventional deployment of U.S. military personnel abroad. This research indicates that seven conditions exist in the cyberspace environment that can enhance the conduct of UW. Since no organization in the U.S. military with the requisite capabilities to exploit these conditions in the cyber domain exists, one should be created. Cyber-enabled UW can provide scalable military options to U.S. policymakers that are currently not available.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CBI	China, Burma, and India (theater in WWII)
CIA	Central Intelligence Agency
DDoS	Distributed Denial of Service
DET 101	Service Unit Detachment 101
DODIN	Department of Defense Information Networks
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
IO	Information Operations
NATO	North Atlantic Treaty Organization
OSS	Office of Strategic Services
RBN	Russian Business Network
SF	Special Forces
SFODA	Special Forces Operational Detachment Alpha
SMT	Social Movement Theory
SNA	Social Network Analysis
SOE	Special Operations Executive
SOF	Special Operations Forces
SQL	Structured Query Language
U.S.S.R.	United Soviet Socialist Republics
USCYBERCOM	United States Cyber Command
USSOCOM	United States Special Operations Command
UW	Unconventional Warfare
WWII	World War II

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Given current U.S. reluctance to commit conventional troops and an environment of constrained resources, alternate military strategies to support foreign policy aims are urgently needed. An area that holds the potential for low-profile campaigns to confront enemies of the United States is the application of unconventional warfare (UW) working by, with, and through indigenous groups via cyberspace-based operations or cyber-enabled UW. Conducting military operations through cyber-enabled UW is less expensive and inherently involves less risk than a conventional deployment of U.S. military personnel abroad. Additionally, cyber-enabled UW can provide scalable military options to U.S. policymakers that are currently not available. This thesis will identify and explore conditions that can facilitate the conduct of cyber-enabled UW operations by examining cases in which state and non-state actors mobilized populations in UW-like operations that exploited the cyber domain.

A. SIGNIFICANCE OF RESEARCH

UW has been defined in a number of different ways. For the purposes of this thesis, the U.S. definition of UW will be used as a guiding principle. Under this definition, U.S. forces infiltrate into enemy-held territory to identify, recruit, and operationalize underground, auxiliary, and paramilitary forces toward the purpose of sabotage, subversion, or to overthrow an enemy regime.[1]

[1] Department of the Army, *Army Special Operations Forces* [FM 3-05 (FM100-25)] (Washington, DC: Headquarters, Department of the Army, 2006); Department of the Army, *Army Special Operations Forces Unconventional Warfare* (FM 3-05.130) (Washington, DC: Headquarters, Department of the Army, 2008); Department of the Army, *Special Forces: Unconventional Warfare* (TC 18-01) (Washington, DC: Headquarters, Department of the Army, 2010), https://nsnbc.files.wordpress.com/2011/10/special-forces-uw-tc-18-01.pdf; Joint Chiefs of Staff, *Special Operations* (JP 3-05) (Washington, DC: Joint Chiefs of Staff, 2014), http://dtic.mil/doctrine/new_pubs/jp3_05.pdf; Special Warfare Center and Schools, *A Leader's Handbook to Unconventional Warfare* (SWCS PUB 09-1) (Fort Bragg, NC: Special Warfare Center and School, 2009); U.S. Army Special Operations Command, "ARSOF 2022," *Special Warfare Magazine* 26, no. 2 (April-June 2013); U.S. Army Special Operations Command, "ARSOF 2022 Part 2: Changing the Institution," *Special Warfare Magazine* 27, no. 3 (September 2014); U.S. Army Special Operations Command, "Counter-Unconventional Warfare" (White Paper), September 26, 2014.

The Internet has provided militaries around the world with another domain in which to operate, cyberspace. Over three billion people have access to the Internet, and the number grows each day. It is imperative that Special Operations Forces (SOF) understand how networks operate in this domain to enhance UW. Starting in the 1990s, leading scholars began looking at how networks operate in cyberspace and the objectives they could achieve.[2] This quickly led to the military operationalizing the cyber domain and new areas of study to include cyberwar and cyberspace operations.[3]

The advent of social media in particular has forced the evolution of concepts presented in collective action, social movement theory, and social network analysis into another operational realm, cyberspace. The information revolution has spawned thousands, if not millions, of digital networks. If it is to be successful in the next generation of UW, SOF must be fully prepared to exploit this domain.

While the U.S. military strove to wage two largely conventional military campaigns in Iraq and Afghanistan, adversarial state and non-state actors were perfecting their use of cyberspace-based operations. The Department of Defense defines these operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace," to include both overt and covert

---

[2] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1993): 141–65, doi: 10.1080/01495939308402915; John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001); William C. Boni and Gerald L. Kovacich, *Netspionage: The Global Threat to Information* (Boston: Butterworth-Heinemann, 2000).

[3] John Arquilla and Douglas A. Borer, *Information Strategy and Warfare: A Guide to Theory and Practice* (New York: Routledge, 2007); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Tantor, 2014); Christopher R. Eidman and Gregory S. Green, "Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare" (master's thesis, Naval Postgraduate School, 2014), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA607604; James A. Lewis, "Assessing the Risks of Cyber Terrorism: Cyber War and Other Cyber Threats," Center for Strategic and International Studies, 2002; Dorothy E. Denning, "Cyber Conflict as an Emergent Social Phenomenon," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, ed. Thomas J. Holt and Bernadette H. Schell (Hershey, PA: Information Science Reference, 2011), doi: 10.4018/978-1-61692-805-6; Joseph S. Nye Jr., "Cyber Power," Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (2010): 97–108.

objectives.[4] In 2014, Russia quietly used cyberspace operations to support its annexation of Crimea, sovereign Ukrainian territory. Additionally, the Islamic State has used cyberspace to help recruit a terrorist army and administer a de-facto state. Over the past decade and a half, enemies of the United States have been successfully harnessing the power of Internet technologies to conduct cyberspace operations to enhance recruitment, organize their forces, and execute operations. In order to explore how the United States can update its model of unconventional warfare, we studied the following research question: Under what conditions can cyberspace operations be used to enhance unconventional warfare**?**

1. Claims

We make two general claims. First, the low cost of entry, sparse regulations, and relative anonymity of users in the virtual environment facilitates social mobilization and recruiting of proxy forces during UW cyberspace operations.[5] Second, the speed of transmitting information and the vast amount of multi-media content available makes cyberspace an excellent platform for large social movements, specifically UW resistance groups and their underground support networks, to organize, train, and eventually conduct operations.[6]

---

[4] Joint Chiefs of Staff, *Cyberspace Operations* [JP 3-12 (R)] (Washington, DC: Joint Chiefs of Staff, 2013), http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[5] Damon M. Centola, "Homophily, Networks, and Critical Mass: Solving the Start-up Problem in Large Group Collective Action," *Rationality and Society* 25, no. 1 (February 2013): 3–40, doi: 10.1177/1043463112473734; Mancur Olson *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge: Harvard Univ. Press, 2002); Elinor Ostrom, "A Behavioral Approach to the Rational Choice Theory of Collective Action: Presidential Address, American Political Science Association, 1997," *American Political Science Review* 92, no. 1 (March 1998): 1–22, doi: 10.2307/2585925; Elinor Ostrom, "Analyzing Collective Action," *Agricultural Economics* 41 (November 2010): 155–66, doi: 10.1111/j.1574-0862.2010.00497.x; Elinor Ostrom, "Collective Action and the Evolution of Social Norms," *Journal of Natural Resources Policy Research* 6, no. 4 (2014): 235–52, doi: 10.1080/19390459.2014.935173.

[6] Doug McAdam, John D. McCarthy, and Mayer N. Zald, *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings* (Cambridge: Cambridge Univ. Press, 1996); Doowan Lee and Glenn W. Johnson, "Revisiting the Social Movement Approach to Unconventional Warfare," *Small Wars Journal*, December 1, 2014, http://smallwarsjournal.com/jrnl/art/revisiting-the-social-movement-approach-to-unconventional-warfare; Doowan Lee, "A Social Movement Approach to Unconventional Warfare" *Special Warfare* 26, no. 3 (September 2013) 27–32; Karl-Dieter Opp, *Theories of Political Protest and Social Movements: A Multidisciplinary Introduction, Critique, and Synthesis* (London: Routledge, 2009).

B. METHODOLOGY

The main body of the research will utilize an exploratory design to provide evidence in support of the claims stated in the previous section. We will accomplish this through an analysis of information at the empirical level. We will also employ a comparative case study analysis to identify conditions explaining our proposed outcomes. We have identified four cases to inform and guide our research: 1) Service Unit Detachment 101's use of proxy forces and UW techniques in Burma during World War II; 2) Russia's use of cyber-enabled operations against the Republic of Georgia; 3) Russia's use of cyberspace operations against Crimea and the Ukraine, 4) Al Suri's *Global Islamic Resistance Call* and the Islamic State's employment of it, which illustrates non-state actor use of the Internet for the purposes of recruiting, training, and executing operations. These case studies were selected for our research because Service Unit Detachment 101 is often touted as one of the most successful UW operations conducted in WWII and provides a pure example of UW tactics, techniques, and procedures. Additionally, the Russian and non-state actor case studies were selected because they are some of the most current instances of exploitation of the cyber domain to conduct UW-like operations. The basic scenario and significance of each of these case studies will be expanded upon in the next section.

After conducting a UW literature review (Chapter II) and analysis of a classic U.S. UW operation, Service Unit Detachment 101 (Chapter III), the following four activities—recruitment, indoctrination, training, and operationalizing proxy forces—were determined to be required for a successful UW operation. The research will examine two areas of knowledge: social mobilization and cyberspace operations through the lens of the four activities (recruiting, indoctrinating, training, and operationalizing proxy forces) to identify conditions that enhance UW. The first part of the research will provide the base theoretical underpinnings to support how UW, as a subset of social mobilization, can utilize conditions provided by information age technologies (particularly digital and Internet platforms) to enhance operations in cyberspace. In this bin of research, collective action theory, social movement theory, social network analysis (particularly analysis of dark networks), and UW doctrine will be considered.

1. Conceptual Framework

The conceptual framework for this thesis is broken down into three major areas of study. The first area of study is unconventional warfare and the hallmarks of a successful U.S. UW operation. The second area of study is the social mobilization of populations. The final area of study focuses on case studies of UW-like operations that utilized cyberspace operations.

a. Unconventional Warfare and Hallmarks of Successful UW

The UW area of study will define UW and use the Service Detachment Unit 101 case study to examine and extract details pertinent to successful techniques for recruiting, training, and operationalizing proxy forces.[7] The Department of Defense defines unconventional warfare as "[activities] conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[8] Within the U.S. military, U.S. Army Special Operations is designated as the primary organization to conduct UW. As such, U.S. Army Special Operations has identified UW as being composed of seven phases: preparation, initial contact, infiltration, organization and training, build-up, employment, and transition.[9] Service Detachment Unit 101 is often touted as one of the most successful U.S. UW operations

---

[7] Steven J. Cox, "Role of SOF in Paramilitary Operations" (master's thesis, Naval Postgraduate School, 1995), http://calhoun.nps.edu/handle/10945/31295; Roger Hilsman, *American Guerrilla: My War behind Japanese Lines* (Nebraska: Potomac Books, 1990); Derek Jones, "Ending the Debate: Unconventional Warfare, Foreign Internal Defense, and Why Words Matter" (master's thesis, U.S. Army Command and General Staff College, 2006), http://ftp.fas.org/man/eprint/jones.pdf; Richard D. Newton et al., *Contemporary Security Challenges: Irregular Warfare and Indirect Approaches* (Hurlburt Field, FL: Joint Special Operations Univ. Press, 2009); Troy James Sacquety, "The Organizational Evolution of OSS Detachment 101 in Burma, 1942–1945" (doctoral dissertation, Texas A&M Univ., 2008), http://repository.tamu.edu/bitstream/handle/1969.1/ETD-TAMU-3280/SACQUETY-DISSERTATION.pdf ?sequence=1&isAllowed=y; John J. Tierney Jr., *Chasing Ghosts: Unconventional Warfare in American History* (Washington, DC: Potomac, 2006); Randall D. Wenner, "Detachment 101 in the CBI: An Unconventional Warfare Paradigm for Contemporary Special Operations" (master's thesis, U.S. Army Command and General Staff College, 2010), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix= html&identifier=ADA523185.

[8] Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms* (JP 1-02) (Washington, DC: Joint Chiefs of Staff, 2010), 263, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[9] Department of the Army, *Special Forces* (TC 18-01), 1-8–1-9.

and was conducted in WWII. This case study will illustrate UW tactics, techniques, and procedures prior to the advent of cyberspace operations and Internet technologies.

b. Social Mobilization of Populations

To understand the social mobilization area of study, investigation into three theoretical underpinnings is necessary: collective action, social movement theory, and social network analysis. The first subcategory of this group of research is collective action, which explains why individuals establish groups and organizations for common causes.[10] Of particular interest to this research is the "start-up problem" and what motivates individuals to move past selfish motivation and engage in collective behavior.[11]

Related to collective action is the second subcategory, social movement theory (SMT). The concepts contained in the SMT literature connect micro-level (individual) incentives to macro-level (societal) events.[12] The study of social movements provides SOF with an understanding of how large groups of individuals can come together to make major changes in society, a critical piece in any UW campaign.

---

[10] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge: Harvard Univ. Press, 2009); Damon M. Centola, "Homophily, Networks, and Critical Mass: Solving the Start-up Problem in Large Group Collective Action," *Rationality and Society* 25, no. 1 (February 2013): 3–40, doi: 10.1177/1043463112473734; Roger V. Gould, "Collective Action and Network Structure," *American Sociological Review* 58, no. 2 (April 1993), doi:10.2307/2095965; Gerald Marwell, Pamela E. Oliver, and Ralph Prahl, "Social Networks and Collective Action: A Theory of the Critical Mass. III," *American Journal of Sociology* 94, no. 3 (1988): 502–34; Brian Petit, "Social Media and UW," *Special Warfare Magazine* 25, no. 2 (2012), http://www.soc.mil/swcs/swmag/archive/SW2502/SW2502SocialMediaAndUW.html.; Aldon Morris, "Reflections on Social Movement Theory: Criticisms and Proposals," *Contemporary Sociology* 29, no. 3 (May 2000): 445, doi: 10.2307/2653931; Pamela E. Oliver, "Formal Models of Collective Action," *Annual Review of Sociology* 19, (1993): 271–300; Elinor Ostrom, "A Behavioral Approach to the Rational Choice Theory of Collective Action: Presidential Address, American Political Science Association, 1997," *American Political Science Review* 92, no. 1 (March 1998): 1; Elinor Ostrom, "Analyzing Collective Action," *Agricultural Economics* 41, no. s1 (November 2010): 155–66; Ostrom, "Collective Action and the Evolution."

[11] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge: Harvard Univ. Press, 2009).

[12] Doug McAdam, John D. McCarthy, and Mayer N. Zald, *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings* (Cambridge: Cambridge Univ. Press, 1996); Aldon D. Morris and Carol McClurg Mueller, *Frontiers in Social Movement Theory* (New Haven, CT: Yale Univ. Press, 1992); Melissa Y. Lerner, "Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt," *Journal of Muslim Minority Affairs* 30, no. 4 (December 2010): 555–74; Morris, "Reflections on Social Movement Theory," 445; Karl-Dieter Opp, *Theories of Political Protest*.

The third subcategory concerning the mobilization of populations is social network analysis (SNA). This area of research digs deeper into existing networks to determine relationships between their various, and sometimes disparate, members.[13] A critical subset of this research is the analysis of dark networks.[14] Dark networks are primarily viewed as criminal and terrorist networks.[15] Exiled resistance groups, necessary for UW, are also considered dark networks because they attempt to keep their membership hidden.[16]

c. Conceptual Diagram

In order to illustrate in each of the case studies the conditions present in successful cyber-enabled UW-like operations, the following framework for analysis depicted in Figure 1 is used:

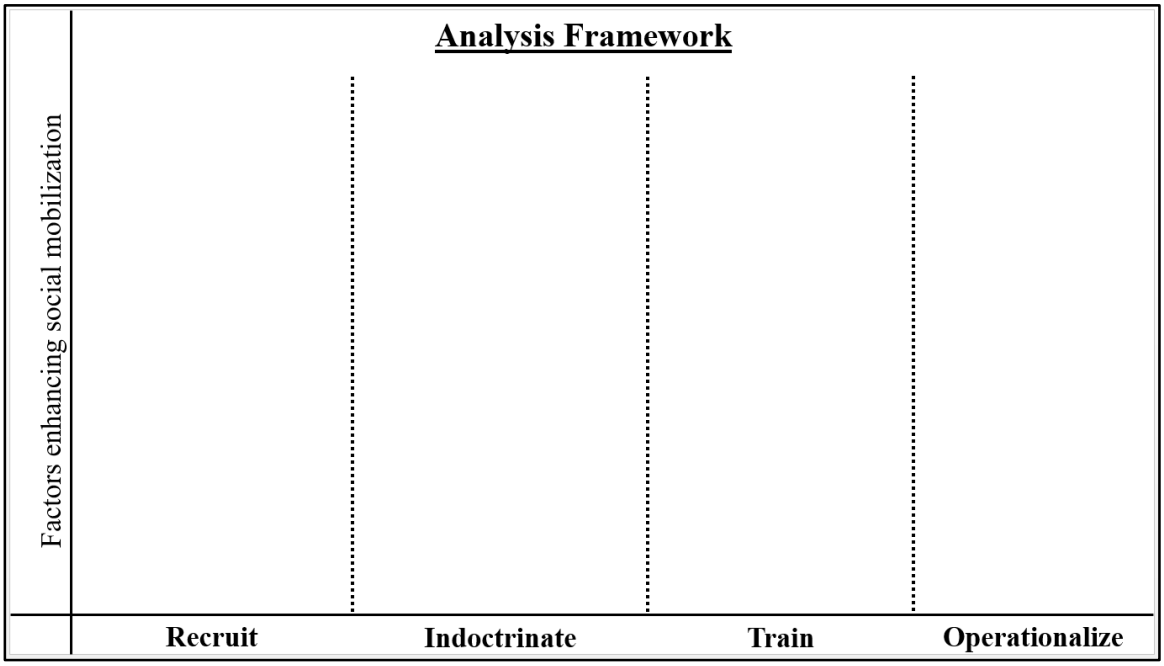
[13] Kirk A. Duncan, "Assessing the Use of Social Media in a Revolutionary Environment" (master's thesis, Naval Postgraduate School, 2013), http://calhoun.nps.edu/handle/10945/34660; Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge Univ. Press, 2012); Christina Prell, *Social Network Analysis: History, Theory and Methodology* (London: SAGE, 2012); René M. Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience," *Journal of Policy Analysis and Management* 31, no. 1 (winter 2012): 33–62, doi: 10.1002/pam.20619; Sean S. Everton, "Tracking, Destabilizing and Disrupting Dark Networks with Social Networks Analysis" (Version 1.05), Naval Postgraduate School, 2008, http://calhoun.nps.edu/handle/10945/34415 Mark S. Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78, no. 6 (May 1973): 1360–80; Michael McBride and David Hewitt, "The Enemy You Can't See: An Investigation of the Disruption of Dark Networks," *Journal of Economic Behavior & Organization* 93 (September 2013): 32–50, doi: 10.1016/ j.jebo.2013.07.004; Nancy Roberts and Sean F. Everton, "Strategies for Combating Dark Networks," *Journal of Social Structure* 12, no. 2 (2011): 1–32, http://calhoun.nps.edu/public/handle/10945/41260.

[14] Ibid.

[15] Ibid.

[16] Ibid.

Figure 1. Analysis Framework



Across the bottom of the diagram are the four activities, recruiting, indoctrinating, training, and operationalizing, which are identified in the UW literature review and Service Unit Detachment 101 case study and will be analyzed in-depth. On the left hand side, factors enhancing social mobilization will identify the techniques used within each of the four categories. Each column will be filled with examples from the case studies.

2. Case Studies

To date, no state or non-state actor has publicly acknowledged (or published) a formal model of cyber-enabled UW. As such, conditions necessary for the execution of UW through cyberspace operations must be extracted from historical examples in which state and non-state entities use information age technologies for recruiting, indoctrinating, training, and executing UW-like operations.

a. Service Unit Detachment 101

During World War II, the United States conducted a wide variety of special operations, including UW. In many of these campaigns, limited success was achieved.

One noted exception to this rule is Service Unit Detachment 101's (DET 101) operations in Burma. Prior to examining case studies pertaining to how both state and non-state actors have used cyber-enabled capabilities to enhance and execute UW-like operations, it is prudent to examine an example of successful UW prior to the advent of the Internet and other information age technologies.

b. Russia versus Georgia: The South Ossetia Campaign

In its 2008 campaign to annex South Ossetia, Russia, used military force in order to take territory and further their perceived national security interests, disregarding the borders of sovereign nations.[17] In addition to conventional warfare, there is evidence that Russia also employed a massive cyber-attack and information warfare campaign. Although Russia denies any involvement in the cyber and propaganda warfare that was executed in close proximity with (and in preparation for) conventional operations, closer scrutiny indicates that there was coordination between "hacktivists" and organized criminal organizations.[18]

---

[17] Jolanta Darczewska, "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study," OSW Point of View, vol. 42, Centre for Eastern Studies, May 2014.

[18] Robert M. Cutler, "Russia's Disinformation Campaign over South Ossetia," *Central Asia-Caucasus Institute Analyst* 10, no. 16 (August 2008): 6–8; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (February 2012): 3–24, doi: 10.1177/0967010611431079; James P. Farwell, and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011): 23–40, doi: 10.1080/00396338.2011.555586; George Friedman, "The Russo-Georgian War and the Balance of Power," *Stratfor*, August 12, 2008, http://blog.cafewall.com/wp-content/uploads/2008/09/rus-v-geo-analysis.pdf; Valery Gerasimov, "The New Generation Warfare," *VPK News*, March 27, 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf; Keir Giles, "'Information Troops'-A Russian Cyber Command," proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, June 7–10, 2011, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5954699; Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence," *Communications of the ACM* 54, no. 8 (August 2011): 132–40, doi: 10.1145/1978542.1978569; David Hollis, "Cyber War Case Study: Georgia 2008," *Small Wars Journal* 7, no. 1 (January 2011); Athina Karatzogianni, "Blame it on the Russians: Tracking the Portrayal of Russians During Cyber conflict Incidents," *Digital Icons: Studies in Russian, Eurasian and Central European New Media* 4 (2010): 128–50; Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (winter 2008–9): 60–76; Marian Lazar, "Russian Cyber Campaign against Georgia," In *The Complex and Dynamic Nature of the Security Environment* (Bucharest, Romania: National Defense Univ., 2012), 500–6; Paolo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," *Military Review* 91, no. 6 (November-December 2011): 63–68; Timothy L. Thomas, "The Bear Went through the Mountain: Russia Appraises its Five-Day War in South Ossetia," *Journal of Slavic Military Studies* 22, no. 1 (2009): 31–67, doi: 10.1080/13518040802695241.

In this new form of information warfare, Russia is now utilizing old propaganda techniques, from the days of the Soviet Union, packaged in new age technologies (particularly Internet-based social media).[19] The 2008 Russia-Georgia conflict is significant because it provides an example of a highly sophisticated operation in the cyber-domain with results that manifested in the real world.

c. Russia versus Ukraine: The Crimea Annexation

In February 2014, Russia used cyberspace operations to initiate an unconventional warfare campaign against Crimea that severed the Ukrainian military and security services command and control capabilities resulting in the ultimate annexation of Crimea by Russia.[20] Additionally, as the operation was being conducted, Russia employed numerous information warfare techniques including cyberattacks, propaganda and deception operations using proxy Internet "troll armies" and numerous social media platforms to enhance and garner support for its UW paramilitary forces operating within Ukraine.[21]

This case study may be the most important in seeking an answer to the research question of this thesis, as Russian cyberspace operations were conducted as part of a successful UW operation, the annexation of Crimea. Furthermore, Russia continues to adapt, refine and conduct cyberspace operations to assist its UW efforts in eastern Ukraine, providing current techniques, tactics, and procedures for analysis.

d. Non-state Actors

The use of the Internet by non-state actors, particularly terrorist organizations, is not a new occurrence. In fact, by the turn of the last century, nearly all terrorist organizations, both foreign and domestic, began to use and exploit the Internet for a

---

[19] Daisy Sindelar, "Inside Russia's Disinformation Campaign," *Atlantic*, August 12, 2014, http://www.defenseone.com/technology/2014/08/inside-russias-disinformation-campaign/91286/.

[20] Michael R. Gordon, "Russia Displays a New Military Prowess in Ukraine's East," *New York Times*, April 21, 2014, http://www.nytimes.com/2014/04/22/world/europe/new-prowess-for-russians.html?_r=0.

[21] Ibid.; Sindelar, "Inside Russia's Disinformation Campaign."

variety of purposes.[22] An examination of Al Suri's *Global Islamic Resistance Call*, which he published in 2004, reveals a blueprint for how Al-Qaeda should train and conduct operations. It also shows how the Internet should serve as a platform for this as well as a way to reach a mass audience.[23] Al-Suri established the foundation currently used by the Islamic State, which has become the poster child for how terrorist organizations can conduct de-centralized global UW activities, including recruiting, training, and executing operations using cyberspace as a platform.[24]

C. THESIS OVERVIEW AND OUTLINE

The remainder of the thesis is organized as follows: Chapter II discusses theories relevant to the mobilization of populations, specifically collective action, social movement theory, and social network analysis, and the roles of these theories in UW. Chapter III describes unconventional warfare and uses the "Service Detachment Unit 101" case study to identify successful techniques for the recruiting, indoctrinating, training, and operationalizing proxy forces. Additionally, Chapter III covers the other three case studies outlined above. Chapter IV contains our analysis and the conditions necessary for cyberspace operations to enhance UW in relation to recruitment, indoctrination, training, and operationalizing proxy forces. Chapter IV also provides the authors recommendations for the creation of a cyber-enabled UW team. Finally, Chapter V provides the authors' conclusions and suggestions for future inquiry and research.

---

[22] Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet" Special Report 116, United States Institute of Peace, March 2004, http://books.google.com/books?hl=en&lr=&id=a_cugt6quTYC&oi=fnd&pg=PA2&dq=%22of+the+World+Wide%22+%22Terrorism+on+the+Internet+is+a+very+dynamic+phenomenon:+websites+suddenly%22+%22uses+made+of+the+Internet.+Those+uses+are+numerous+and,+from+the%22+&ots=JiC6c1Iry2&sig=taVdPF__glV5ba6ru6MjQBSFNZ4.

[23] Paul Cruickshank and Mohanad Hage Ali, "Abu Musab Al Suri: Architect of the New Al Qaeda," *Studies in Conflict & Terrorism* 30, no. 1 (January 2007): 1–14, doi: 10.1080/10576100601049928; Jim Lacey, *A Terrorist's Call to Global Jihad: Deciphering Abu Musab Al-Suri's Islamic Jihad Manifesto* (Annapolis, MD: Naval Institute, 2008); Brynjar Lia, *Architect of Global Jihad: The Life of Al-Qaida Strategist Abu Mus'ab Al-Suri* (London: Hurst, 2014); M. W. Zackie, "An Analysis of Abu Mus'ab Al-Suri's 'Call to Global Islamic Resistance,'" *Journal of Strategic Security* 6, no. 1 (March 2013): 1–18, doi: 10.5038/1944-0472.6.1.1.

[24] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SOCIAL MOBILIZATION

In order to identify and understand critical factors necessary for the successful execution of cyber-enabled UW, the key concepts of theories of social mobilization need to be extracted. UW is in essence a form of social mobilization in order to obtain a strategic objective in a target country. This section will first examine the history and current U.S. doctrine related to UW. The second section will examine the cyber-domain and how it relates to UW and social mobilization. The next three sections will present a brief review of three theories, collective action theory, social movement theory (SMT), and social network analysis (SNA), to summarize key aspects of the theory and extract critical concepts. The final section will analyze the theories and attempt to find commonalities between critical ideas.

A. UNCONVENTIONAL WARFARE

The United States Army Special Operations Command has recently placed additional emphasis on examining UW as a strategic option for policy makers. Although UW has been recently highlighted, it is by no means a new or innovative technique. Looking solely at the U.S. history of using this form of warfare, its origins can be traced back to before the Declaration of Independence was even signed. Prior to the conflicts in Iraq and Afghanistan, at least sixteen American conflicts have included elements of warfare that could be labeled unconventional in nature.[25]

American UW doctrine and theory was primarily extracted from U.S. and Allied actions conducted in World War II (WWII). These operations were initially conducted under the purview of the Special Operations Executive (SOE) and Office of Strategic Services (OSS) and primarily included strategic support of resistance groups and

[25] Tierney, *Chasing Ghosts*.

sabotage missions in occupied Europe and Asia.[26] The two most noteworthy efforts of these groups (and arguably most successful) were the Jedburghs operations in occupied France and Detachment 101's operations in Burma.[27]

According to the Department of Defense's *Dictionary of Military and Associated Terms*, UW is defined as "[activities] conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[28] U.S. Army Special Operations additionally identifies seven phases of UW: preparation, initial contact, infiltration, organization and training, build-up, employment, transition.[29]

Throughout the years, UW has been referred to using many different monikers including guerrilla warfare, insurrectionary warfare, revolutionary warfare, and even class warfare.[30] It is also regularly confused with irregular warfare, which (according to the U.S. definition) is an umbrella term for any operation that involves a conflict between a state and a counter-state.[31] Within irregular warfare, there are five types of activities, one of which is UW. The other four include activities where U.S. forces support a state against a counter-state: Foreign Internal Defense, Security Force Assistance, Counter Terrorism, and Counter Insurgency. UW represents the one activity where the United States would support the efforts of a counter-state against the state.[32]

---

[26] Will Irwin, *The Jedburghs: The Secret History of the Allied Special Forces, France 1944* (New York: PublicAffairs, 2009); Alfred H. Paddock Jr., *US Army Special Warfare, Its Origins: Psychological and Unconventional Warfare, 1941–1952* (Honolulu: Univ. Press of the Pacific, 2002), http://books.google.com/books?hl=en&lr=&id=3pWi0xfw6q0C&oi=fnd&pg=PR9&dq=%22Coordinator+of+Information%22+%22of+OSS%22+%22Joint+Subsidiary+Plans+Division%22+%22and+Unconventional+Warfare%22+%22Office+of+Policy+Coordination%22+%22Propaganda+Branch,+G-2%22+%22Assistance+to%22+%22Toward+Unconventional+Warfare%22+%22and+Psychological+Warfare+in+Korea%22+&ots=0G4XrxhtgR&sig=IXbLGndXBHKQGUScb8XvCOU_uDY..

[27] Ibid.

[28] Joint Chiefs of Staff, *Dictionary of Military and Associated Terms* (JP 1-02), 263.

[29] Department of the Army, *Special Forces* (TC 18-01), 1-8–1-9.

[30] Andrew C. Janos, "Unconventional Warfare: Framework and Analysis." *World Politics* 15, no. 4 (July 1963): 636–46. doi:10.2307/2009460.

[31] Joint Chiefs of Staff, *Dictionary of Military and Associated Terms* (JP 1-02), 134.

[32] Joint Chiefs of Staff, *Special Operations* (TC 18-01), II-1–II-18.

The U.S. Army identifies seven phases of UW. The first phase of UW is preparation, which includes intelligence, operational, and psychological preparation of the environment for unconventional warfare. The second phase is initial contact with resistance groups or governments in exile. The third phase is infiltration of U.S. forces into denied or occupied territory to link-up with resistance groups. The fourth phase is organizing and training of resistance groups into inactive support, active support, and armed groups. The fifth phase is the building-up of the capacity and capability of resistance organizations. The sixth phase is employment of resistance groups. This phase lasts until active conflict ends or the fight is transitioned to be executed using conventional means. The seventh and final phase is transition in which armed resistance groups are either stood down, or transitioned into security forces of the new government.[33]

Although there are many tasks and sub-tasks contained in the seven phases of UW, through our literature review we identified are four critical activities that most influence the success of organizations attempting to conduct warfare through proxy groups. The first of these is the recruitment of suitable participants. This activity occurs in the first through third phases of UW.[34] The second activity is indoctrination, or reinforcing the message and underlying motivation behind the UW campaign. This activity takes place primarily in the third through fifth phase of UW, but will also continue through the entire life of the resistance group.[35] The third activity is training of proxy forces. By definition, training is conducted in the fourth phase of UW, but also continues through the fifth and sixth phase.[36] The final activity is operationalization of the counter-state group. This activity is associated with the sixth phase of UW.[37]

The risks of joining an active insurgency are inherently very high. Counter-state groups start very small and must overcome challenging obstacles if they are to achieve

[33] Department of the Army, *Special Forces* (TC 18-01), 1-8–1-9.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

any measure of success. Many factors must be present for an individual to overlook these risks and literally place their life on the line for a political or military movement. Collective action theory analyzes why individuals coalesce into groups, sometimes despite the rewards or risks that might be present.

B. THE CYBER DOMAIN

Social mobilization, through traditional websites, blogs, social media, and all other manor of platforms, is a persistent and prevalent phenomenon in the digital world. The use of these platforms also falls within the spectrum of cyberspace operations as defined by U.S. doctrine.[38] The low cost of entry, sparse regulations, ease of anonymity and secrecy, the speed of information, and wide availability of multimedia content make the Internet a conducive environment for growing and cultivating resistance organizations.[39]

In their influential 1993 paper, "Cyberwar is Coming!" Arquilla and Ronfeldt noted that the information revolution brought into being technologies that would have profound impacts on the nature of warfare. They introduced the concepts of cyberwar and netwar.[40] They later expanded on the ideas of this original paper in their book *Networks and Netwars*, and introduced the influential idea that future conflicts will primarily be fought between networks and networked organizations, and traditional hierarchies will struggle to compete in this environment.[41]

Cyber warfare is often imagined as complicated hacking schemes to steal data, attacks to corrupt and degrade an opponent's command and control infrastructure, or even perhaps infect the systems of critical online infrastructures.[42] It can also be classified as form of low intensity conflict, where propaganda and social influence

---

[38] Joint Chiefs of Staff, *Cyberspace Operations* [JP 3-12 (R)].

[39] Weimann, "How Modern Terrorism Uses the Internet." Portions also extracted from "Conflict in the Information Age" course paper entitled "The anatomy of online recruitment," by Ryan Gladding.

[40] Arquilla and Ronfeldt, "Cyberwar Is Coming!" 141–65.

[41] Arquilla and Ronfeldt, *Networks and Netwars*, ix–xii.

[42] Goel, "Cyberwarfare," 132–140.

techniques are garnered to bolster support for a social or political cause. This new realm of conflict has important implications for the conduct of both insurgency and counter-insurgency warfare.[43]

Activities associated with cyber-enabled UW include identifying, contacting, training, building, and operationalizing resistance groups through social media, blogs, and websites. Key insurgency leaders can be identified and cultivated without ever deploying U.S. troops to hostile areas. Additionally, online armies with the capabilities to sabotage critical communications can be recruited, trained, and mobilized. Propaganda, psychological, and information operations can be utilized to shape public and international perceptions, all within the digital realm. A discussion of social mobilization will provide the theoretical base to discuss the activities (identified above) pertaining to proxy warfare and cyber-enabled UW.

C. COLLECTIVE ACTION

Collective action theory principally examines the micro-level of group actions. It essentially explains individual motivations to join groups to produce mutual rewards. Other factors lead to group formation, particularly when social change, and not financial reward, is the desired goal. Revolutionary group activity is a core consideration of UW. Given this fact, understanding individuals' internal motivations to join and become productive members of groups is critically important.

Prior to 1965, most social scientists assumed that individuals with common or shared interests would likely group together to obtain common goals. The theory held that, individual interests and group interests are generally linked and there is little difference between the two.[44] In 1965, an economist, Olson, presented an argument in opposition to this concept. Olson stated that if there is no way for the collective rewards of group membership to be withheld, then individuals in the group have no motivation to

[43] Samuel Liles, "Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency," proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, June 7–10, 2011, 47–57, https://ccdcoe.org/publications/2010proceedings/Liles%20-%20Cyber%20warfare%20%20As%20a%20form%20of%20low-intensity%20conflict%20and%20insurgency.pdf.

[44] Oliver, "Formal Models of Collective Action," 272–75.

contribute. This causes a problem, in which members have the ability to contribute little or nothing to the group's objectives, while still being able to reap the rewards obtained by the group. This is termed the "free-rider" problem in collective action.[45] From Olson's and others' research (particularly that of Ostrom), six factors can be identified as helping to overcome the free-rider problem and therefore increase the likelihood for collective action.[46]

The first factor affecting collective action is group size. Moderately sized groups are most able to overcome collective action problems and therefore should be the core of a UW network. As the size of the group increases, the cost (in resources) of maintaining the group also increases. Additionally, in large groups identifying the contributions of individual members and coming to agreements regarding group strategy is significantly more challenging.[47] On the other side of the argument, very small groups cannot easily generate the resources necessary to achieve their objectives effectively.[48]

The second factor affecting collective action is resource distribution. How group revenues are distributed can influence an individual's motivation to engage in collective action and should be a factor considered by leadership within a resistance organization. If group returns are divided evenly among members, it increases the tendency of members in larger groups to free ride. If benefits are not divided equally, and are instead pooled and then distributed to members, other issues (related to group size may) arise, particularly disputes over equal distribution.[49]

UW organizations have historically been uniquely equipped to interact and communicate with diverse cultures. The third factor affecting collective action is how group heterogeneity, including common interests, ideas, culture, language, or other factors can lead an individual to engage in collective action, even if the payoff for group participation is less than desired. Identifying and exploiting heterogeneous groups is

[45] Olson, *Logic of Collective Action*.

[46] Ibid.

[47] Ibid.

[48] Ostrom, "Analyzing Collective Action," 157.

[49] Ibid.

likely to be a major contributing factor in overcoming the free-rider issue as insurgent groups grow larger.[50]

Traditional UW organizations have relied on small groups to effect personal communications with potential resistance groups. The fourth factor, personal, or face-to-face, communication is shown to be a contributor to overcoming collective action dilemmas. This effect is due to non-verbal communication's potential to increase trust between group participants, thereby increasing the potential for group participation.[51] Advances in digital communication technologies, including video teleconferencing and potentially even virtual reality, will mitigate negative effects previously associated with distant communication techniques.

Two additional factors of collective action should be carefully considered by UW planners when developing individual networks. These involve what information a prospective group member has regarding the group's previous actions and the nature of how the network is linked together. The fifth factor indicates that the more information an individual has on the group's past, the more likely they will be to engage in collective action.[52] The sixth encompasses how members of the group are linked together including both their strong, weak, internal, and external ties. Social ties can bring members into the group or dispel members from it. These ties can also indicate how information, resources, and benefits move through the network..[53]

These six factors are applicable to developing interactions that will lead to a social model of collective action and contribute to the success of any UW activity. Contained within these factors are several core concepts. These concepts are trust, reciprocity, and reputation.[54] Trust between all members is a key variable in group behavior. If trust disintegrates then the social interaction will likely soon follow.

---

[50] Centola, "Homophily, Networks, and Critical Mass," 3–40; Ostrom, "Analyzing Collective Action," 158.

[51] Ostrom, "Analyzing Collective Action," 158.

[52] Ibid.

[53] Centola, "Homophily, Networks, and Critical Mass"; Granovetter, "Strength of Weak Ties," 1360–80; Ostrom, "Analyzing Collective Action."

[54] Ostrom, "Behavioral Approach."

Reciprocity between individuals, particularly in the area of trust, will eventually lead to a positive reputation of the group. The status of a group is a crucial element in increasing the likelihood that collective action will happen, and it will additionally improve the chances for sustained collective action.[55]

D. SOCIAL MOVEMENT THEORY

Since it is unlikely that a UW operation will seek to create a new revolutionary organization by incentivizing individuals, another theory needs to be examined to determine external factors that influence a group's productivity. Social movements are a particular form of collective action that are brought into being by societal pressures or the desire to change some aspect of oppressive state control.[56] McAdam, a leading scholar on social movements, roughly defines them as "loosely organized, loosely coordinated, sustained struggles to promote or resist change that rely at least in part on unconventional tactics, and unconventional forms of collective action."[57]

The ability to understand the underlying motivations for social resistance, particularly given that recent social movement groups are relying more heavily on digital technologies, is important to the study of cyber-enabled UW. Recent uprisings, particularly in Tunisia and Egypt, demonstrated an increasing reliance on information age technologies to control and coordinate the actions of social movement groups. Through this use of technology, revolutionary groups have been able to coordinate to levels that have not been seen in previous social movements.[58]

There are three factors that influence the appearance and progress of social movements:

---

[55] Ostrom, "Behavioral Approach"; Ostrom, "Analyzing Collective Action"; Ostrom, "Collective Action and the Evolution," 235–52.

[56] Morris, "Reflections on Social Movement Theory," 445.

[57] Doug McAdam, "Social Movements and Conflicts," Naval Postgraduate School, 2010.

[58] Jeffrey Ghannam, "Social Media in the Arab World: Leading up to the Uprisings of 2011," Center for International Media Assistance, February 2011, http://www.databank.com.lb/docs/Social%20Media%20in%20the%20Arab%20World%20Leading%20up%20to%20the%20Uprisings%20of%202011.pdf; Regina Salanova, "Social Media and Political Change: The Case of the 2011 Revolutions in Tunisia and Egypt," Working Paper no. 2012/7, International Catalan Institute for Peace, December 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2206293.

> (1) [The] structure of political opportunities and constraints confronting the movement; (2) the forms of organization (informal as well as formal), available to insurgents; and (3) the collective process of interpretation, attribution, and social construction that mediate between opportunity and action… [or]…*political opportunities, mobilizing structures, and framing processes*.[59]

The first factor of social movements, political opportunities, are of vital interest to the UW community. These opportunities are defined by the state and capitalized upon by the counter-state.[60] In this way, the state enacts policies that lead to grievances in the population, or fails to enforce policies that would prevent grievances. If these erosions of the relationship between the state and the population become large enough, it causes the state to become vulnerable to insurgent groups. Political opportunities are normally seen to arise in state and counter-state conflicts, but transnational and non-state groups can also capitalize on these opportunities.[61] Growing social connections throughout the world, and the ever-increasing speed of communication, contribute to the transnational nature of political opportunities.

How movements organize and mobilize their resources is particularly important when considering how to recruit, build, and train resistance organizations in the conduct of UW. The second factor significant to the emergence of social movements are mobilizing structures. These structures include how an insurgent or resistance group organizes itself for the purposes of communicating, gaining and distributing resources, obtaining legitimacy, and engaging in collective action to produce political or societal change. The mobilizing structures can encompass both informal networks (familial, friendship, association, activist, and social media) and formal networks (religious,

---

[59] Doug McAdam, John D. McCarthy, and Mayer N. Zald, "Introduction: Opportunities, Mobilizing Structures, and Framing Processes — toward a Synthetic, Comparative Perspective on Social Movements," in *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, ed. Doug McAdam, John D. McCarthy, and Mayer N. Zald (Cambridge Univ. Press, 1996), 2.

[60] Ibid., 3.

[61] Sidney Tarrow, "States and Opportunities: The Political Structuring of Social Movements," in *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, ed. Doug McAdam, John D. McCarthy, and Mayer N. Zald (Cambridge Univ. Press, 1996), 41–61.

professional, protest groups, and social movements).[62] These structures can also be divided into networks that directly support, tacitly support, or do not support the goals of the social movement. The networks that are developed as a part of mobilization is a major contributing factor to the eventual success or failure of the movement..[63]

Narratives and guiding principles are critical factors in the formation and cultivation of resistance organizations. UW professionals need to be well versed in strategic frames as UW networks move from recruitment to operationalization. The third factor is strategic framing. It is how movement groups shape the discriminations and infringements the state, or other opposition group, committed against the movement into a strategic narrative. These statements then become the ideals and principles on which the group is based. Moreover, it is how the group mobilizes the political opportunities into messages that lead to increased legitimacy, recruitment of new members, and counter-state activities.[64] Simplified further, strategic framing is "the conscious strategic efforts by groups of people to fashion shared understandings of the world and of themselves that legitimate and motivate collective action."[65] Additional factors that affect these strategic frames that must be considered include the culture in which they are developed and mobilized, existing counter-narratives or frames, and the impact of the media on the movement's frame.[66]

To further emphasize the relationship between SMT and UW, Lee and Johnson identify the relationship between social movements, social revolutions, and UW. They state that convergence happens when UW operations focus on organizing existing social

---

[62] John D. McCarthy, "Constraints and Opportunities in Adopting, Adapting, and Inventing," in *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, ed. Doug McAdam, John D. McCarthy, and Mayer N. Zald (Cambridge Univ. Press, 1996), 142–51.

[63] Hanspeter Kriesi, "The Organizational Structure of New Social Movements in a Political Context," in *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, ed. Doug McAdam, John D. McCarthy, and Mayer N. Zald (Cambridge, U.K.: Cambridge Univ. Press, 1996), 152–204.

[64] Mayer N. Zald, "Culture, Ideology, and Strategic Framing," in *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, ed. Doug McAdam, John D. McCarthy, and Mayer N. Zald (Cambridge Univ. Press, 1996), 261–74.

[65] McAdam, McCarthy, and Zald, "Introduction," 6.

[66] Ibid.; Zald, "Culture, Ideology, and Strategic Framing."

movements towards the purpose of subverting or replacing a state, rather than attempting to create a new one. This process is inherently easier and cheaper than creating a resistance organization from scratch. Unfortunately, this method relies on the pre-existence of a covert resistance network whose goals align with the objectives of the UW campaign.[67]

The advent of social media and other information age technologies creates additional opportunities to identify covert groups with strategic frames that align with U.S. UW objectives prior to taking the risky step of deploying U.S. personnel into a hostile country. Identifying either strategic frames or political opportunities in a target country can act as a major first step toward developing a viable resistance organization. Utilizing digital technologies, SNA can provide critical insights into potential partner movements.

E. SOCIAL NETWORK ANALYSIS

Networks are everywhere and understanding them is of tantamount importance in the conduct of UW. These include very informal networks of friends, family, and even distant associates. They also include more formal connections among people, such as professional networks and religious networks. These networks can essentially be broken down into the individuals and the ties that connect them together.[68] In contrast to many organizational theories, SNA does not draw a firm distinction between networks and hierarchies. Instead, if a group of individuals, and the relationships between them, can be represented graphically, it is a network.[69]

Understanding and exploiting the relationships between individuals that make up resistance networks will enhance the conduct of UW. Network analysis is primarily concerned with how ties between individuals affect how the network operates. The behavior of the network is not only influenced by direct ties between its members. More

---

[67] Lee, "Social Movement Approach," 29–32; Lee and Johnson, "Revisiting the Social Movement Approach."

[68] Prell, *Social Network Analysis*, 7–9.

[69] Patti Anklam, *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World* (New York: Routledge, 2007), 1–7.

distant ties also seem to affect networks. Secondary, tertiary, and relationships out to the sixth degree (and even further in some cases) can have profound consequences on how the network performs.[70]

The underlying forces that bring resistance networks together and influence their actions are numerous and often times difficult to understand. SNA offers UW planners a tool to gain insight into these social factors that predicate successful counter-state actions. As mentioned earlier, SNA is predicated on many different theories to describe how the relationships between network members influence the actions and ultimately outcomes of the network. These theories are numerous and beyond the scope of this research, but it is useful to expound on some key concepts. First, the value that is gained by individuals joining a network, as well as the value that is produced by the network is referred to as its social capital. Second, trust between network members, including how it is gained and maintained, is also an important concept. Next, social influence is how network members influence the views, beliefs, and actions of other actors in the network. Similarly, social selection seeks to identify how pairs of individuals (or dyads in a social network) are drawn together based on common personality traits or behaviors. Finally, diffusion of innovation explores how ideas and new technologies are transmitted through networks.[71]

Through these theories, SNA seeks to describe and analyze the behavior of the complex and varied social networks that exist in our world. Primarily, it does this through graphically depicting, or visualizing, networks.[72] To do this researchers, or UW professionals, first identify the boundaries of a network they want to analyze. Since most networks can theatrically expand almost infinitely, this is a critical and important first step. Identifying the level of node, or actor, is also important. Networks are often made up of individual people, but can also describe the relationships between small groups,

---

[70] Nicolas A. Christakis and James H. Fowler, *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives*. New York: Back Bay, 2009; Granovetter, "Strength of Weak Ties."

[71] Prell, *Social Network Analysis*, 61–64.

[72] Ibid.

large groups, and even nations. Next, the relationships between actors, or their ties, is a critical factor.[73] Ties can range from direct strong ties to less formal weak ties.[74]

Within the social network the distance, or path, between actors is also important.[75] As mentioned previously, the influence between members that are connected by several degrees can have a more profound impact on that network than would be intuitively thought.[76] The structure, or topography, of the network, particularly how dense or sparse the network is and how dependent it is on a small or larger number of actors, can reveal a lot about its overall behavior. Within the overall topography of the network, subgroups that are connected by strong ties (or cohesive subgroups) can also directly influence how the network behaves.[77]

Identifying key leaders and influential members of resistance organizations is a key task in UW. In most networks, it is clear that some members are more influential than others. SNA seeks to identify these members and how central they are to the overall network. There are a number of algorithms to identify different types of centrality and how they affect the network. Additionally, SNA also seeks to identify key individuals that connect the network together. These important actors are referred to as brokers and bridges.[78] "*Bridges* are ties that span gaps in a social network, whereas *Brokers* are those actors who sit aside a bridge. Both can be seen as being in a position to control the flow of resources through a network.'[79]

SNA helps to identify and visualize what makes networks successful. The networks of primary concern to UW operate in a covert or clandestine manner. For this reason, resistance and insurgent networks are classified as dark networks. Research on

---

[73] Everton, *Disrupting Dark Networks*, 7–9.

[74] Granovetter, "Strength of Weak Ties."

[75] Everton, *Disrupting Dark Networks*, 7–9.

[76] Christakis and Fowler, *Connected: Surprising Power*.

[77] Everton, *Disrupting Dark Networks*, 9–12.

[78] Ibid., 12–13.

[79] Ibid., 13.

dark networks has primarily been focused on how to disrupt them.[80] This research, however, will focus on identifying factors that will help grow, organize, and eventually operationalize counter-state groups.

F. SOCIAL MOBILIZATION

The one method of warfare (UW) and three theories (collective action, SNA, and SMT) described above are all relevant to understanding social mobilization. From this point of view, each theory relates to the internal factors, analysis, or external factors of human social or group behavior. Although significant similarity exists, Table 1 displays where the elements of each theory relate to the activities examined.

Table 1. Factors of Social Mobilization.

UW Research Activities	Unconventional Warfare	Internal (Collective Action)	Analysis (SNA)	External (SMT)
Recruitment	Preparation Initial Contact Infiltration			**Political Opportunities**
Indoctrination	Organization and Training	**Group Size Resource Distribution Group Heterogeneity Ties**	**Boundaries Topography Path/Distance Ties Centrality**	**Mobilizing Structure**
Training				
Operationalization	Build-up Employment	**Personal Communication Past Actions**	**Brokerage**	**Framing Process**

First, collective action relates to factors that cause an individual to be motivated, beyond selfish reasons, to become a part of a communal activity and work toward shared goals. The aspects associated with this theory are categorized as internal social mobilization factors. Next, SNA is used to understand how actors and ties affect group behavior. This is the analysis factor of social mobilization. Finally, SMT seeks to understand what external pressures or group motivations cause networks to form in order

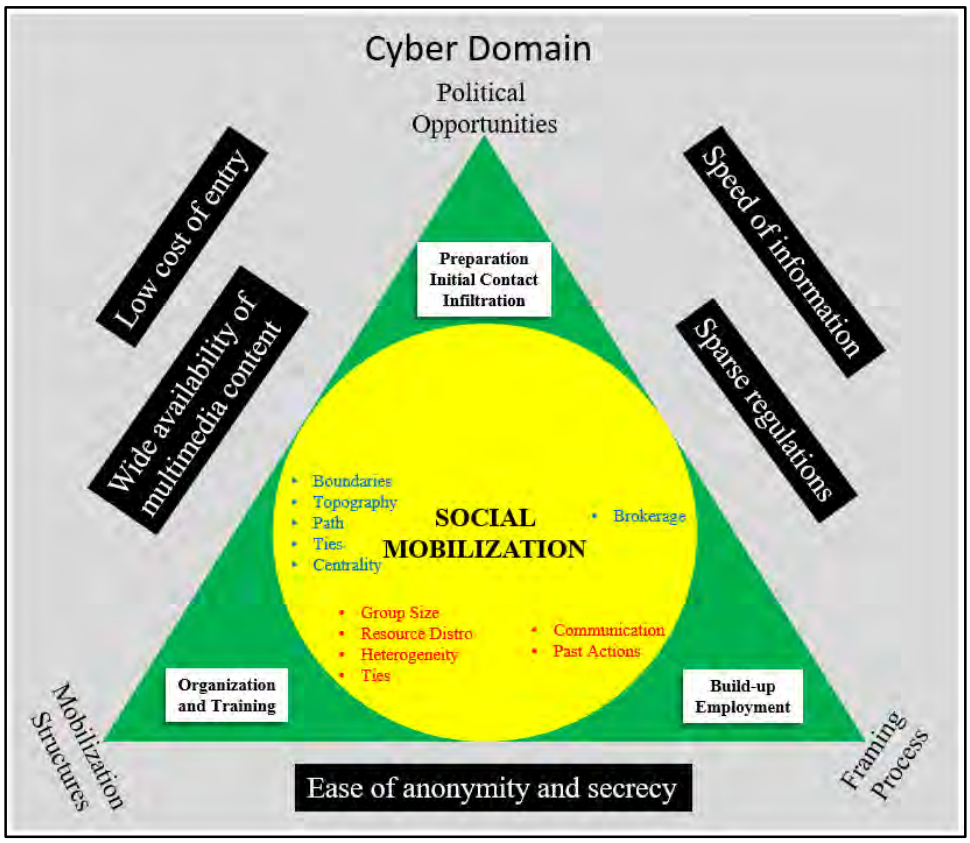
[80] Bakker, Raab, and Milward, "Preliminary Theory of Dark Network," 33–62; Everton, *Disrupting Dark Networks*; Everton, "Tracking, Destabilizing and Disrupting;" Scott Helfstein, "Edges of Radicalization: Ideas, Individuals and Networks in Violent Extremism," U.S. Military Academy, Combating Terrorism Center, February 2012, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA556711; Roberts and Everton, "Strategies for Combating Dark Networks."

to seek social or political changes. These features are classified as external social mobilization factors. Understanding how each theory interacts is critical to identifying the conditions necessary to mobilize resistance groups to conduct unconventional activities.

There are multiple components within each of the research activities, but as indicated in Table 1, there are relationships between these activities, UW as a theory of warfare, and the three theories of social mobilization. Because concepts in all the theories overlap, a true nexus between all of the social mobilization factors would be difficult to determine. Instead, Figure 2 depicts how all of these factors are mutually supporting and should be considered in the goal of mobilizing resistance or insurgent networks.

The figure first depicts cyberspace, and the digital realms that have spawned since the dawn of the information age, as the environment that enhances social mobilization. The black boxes represent conditions in this environment that improve social mobilization in the cyberspace realm. Next, the green triangle represents SMT and the external factors that enhance social mobilization. This portion of the figure also places the phases of UW with their associated external factors at the corners of the triangle. The yellow circle represents the internal processes of social mobilization that improve or help understand group behavior. Within this circle, the red text represents collective action and the blue text represents SNA. Collective action and SNA factors, previously identified in Table 1, are also positioned closest to the external (SMT) factors that they best support.

Figure 2. Cyber-enabled UW



This chapter points out that there is an expansive list of factors that potentially facilitate social mobilization, and particularly the utilization of resistance groups. These factors represent the conditions that greatly enhance the performance of UW in a perfect, theoretical environment. In the real world, it is possible that all of these factors do not need to be present for a counter-state group to be successful. Figure 3 shows that cyber-enabled UW exists in the space at the center of UW, social mobilization, and cyber operations. Even if all of the factors shown in Figure 2 are not present, if UW professionals can identify, exploit, and even manufacture these conditions it will exponentially increase their chance for success.

Figure 3. The Convergence of UW, Social Mobilization, and Cyber Operations

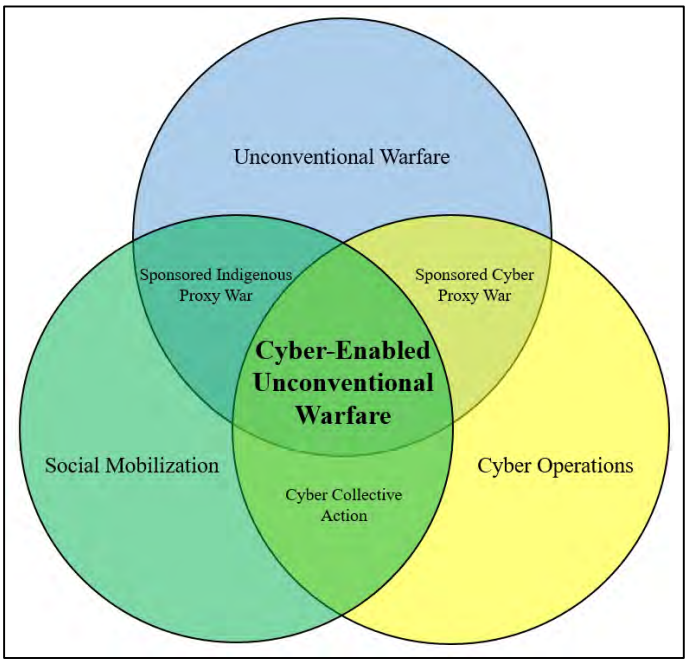


Figure 3 positions cyber-enabled UW at the nexus of UW, social mobilization, and cyber operations. Exploiting cyber-platforms can enhance traditional UW techniques and become a practical, low cost way for the United States to produce social mobilization of counter-state groups. The following chapter will use case studies to identify how these theoretical conditions enhanced operations and ultimately led to the successful prosecution of cyber-enabled UW-like operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES

Four case studies are presented to examine the research activities. The first of these case studies is a pre-information age example and is used to determine that UW tasks can be successfully completed in the absence of information age technologies. This will create a base-line for the UW activities and help to identify what cyber-enabled techniques affect the activities used in this research. The other three cases examine how state and non-state actors exploit conditions in the cyber domain to execute unconventional-like operations.

A. SERVICE DETACHMENT 101

Although China, Burma, and India (CBI) formed a secondary theater in the war, President Franklin D. Roosevelt considered it of great importance, particularly to support the Chinese and keep them in the war against the Japanese. Through the use of UW techniques, Detachment 101 was able to identify, recruit, indoctrinate, and operationalize indigenous proxy forces for the purposes of intelligence gathering, sabotage, subversion, and harassment operations against a numerically superior Japanese enemy. Through these proxy forces, DET 101 was able to inflict severe causalities while sustaining minimal losses to its own force (the casualty rate was approximately 20:1).[81]

This case study of a successful UW organization, operating independent of conventional forces, examines the critical activities of recruiting, indoctrinating, training, and operationalizing proxy forces prior to the advent of information age technologies. It shows that the DET 101 operation in Burma illustrates the techniques and conditions that are necessary for the successful execution of UW. Additionally, it provides an example of how cyber-enabled techniques may enhance traditional UW operations.

This section will first present a history of DET 101's operations in the CBI Theater from 1942 to 1945. This sub-section will relate DET 101 operations to the

[81] Paddock, US Army Special Warfare; Sacquety, "Organizational Evolution of OSS Detachment 101."

modern phases of UW. The second sub-section will analyze the UW activities of recruiting, indoctrinating, training, and operationalizing proxy forces, to determine how DET 101 used tenants of social mobilization, primarily collective action theory and UW doctrine, to achieve positive results. Additionally, this sub-section will explore how cyber-technologies, if they had been available during WWII, could have enhanced the operations and results of this indirect campaign. The final sub-section will offer a summary and present a framework analysis figure for this case study.

1. Background

In 1937, Japanese military forces invaded China and took control of its ports and many major cities. The Japanese pushed forces to the border with India, specifically, they garrisoned units and ran operations out of Myitkyina, to restrict all land resupply into China. This would hinder the Allies from moving supplies and military aid to General Chaing Kai-shek and other Chinese allies. Due to the closed land routes, General Joseph Stillwell, the commander of the CBI Theater, was forced to fly supplies over a route commonly referred to as the "Hump." This air route required pilots to fly a treacherous pass over the Himalayas. Control of these lines of communication (supply routes) became a major theme of all of the campaigns in the CBI Theater. General Stillwell believed that reopening land lines of communication, particularly retaking Myitkyina, was critical to Allied victory in the theater.[82]

General William Donovan, the first head of the OSS, conceived DET 101.[83] Its original purpose was to act as a clandestine intelligence-gathering organization in the Pacific Theater. Organizational infighting and the competing interests of President Roosevelt, General Donovan, General Douglas MacArthur, and General Stilwell precluded the detachment from conducting operations in MacArthur's Southeast Asian

[82] Cox, "Role of SOF," 16.

[83] The Office of Strategic Services (OSS), created in WWII, was the agency responsible for intelligence collection and special warfare operations for the United States. In some ways it mirrored, and was definitely mutually supportive, of Special Operations Europe (SOE). The OSS was decommissioned after WWII, but is credited as the predecessor of both the Central Intelligence Agency (CIA) and modern US Special Operation Command (USSOCOM).

Theater. This eventually led to DET 101's assignment to the CBI Theater under the command of General Stilwell.[84]

Carl Eifler, a young reserve captain, was given command of the detachment. He was recommended for the position by General Stilwell, who ironically did not see a need for an irregular or unconventional capability in his theater. Eifler was given free rein to select personnel for the detachment, train them, and then deploy them to CBI headquarters in New Delhi, India. From there, Eifler pushed DET 101 forward into Burma and established its headquarters at a tea plantation in Nazira after fully integrating his unit and establishing liaison with Stilwell's CBI staff. The Nazira headquarters would act as a base of operations from 1942 to 1945.[85]

Between the formation of DET 101 and its headquarters in Nazira, the purpose and mission of the unit had changed from intelligence collection to a variety of clandestine tasks including sabotage, subversion, espionage, and guerrilla warfare.[86] Although the concept of operational design had not been formalized and named in WWII, the DET 101 staff used many of the elements to plan and execute operations.[87] Through analysis of the tasks and missions given to the unit and liaison with Stilwell's headquarters, it was clear that the Myitkyina area was the Japanese center of gravity. Seizing Myitkyina was key to the operational end state of destroying Japanese forces and reopening land lines of communication into China. Due to the small size of the unit, DET 101 planned to execute a decidedly indirect approach in which they would establish an intelligence network behind enemy lines; recruit, train, organize, and employ a resistance movement; and harass the enemy while simultaneously supporting the efforts of conventional forces operating in the theater.[88]

---

[84] Wenner, "Detachment 101 in the CBI," 10–25.

[85] Cox, "Role of SOF;" Sacquety, "Organizational Evolution of OSS Detachment."

[86] Hilsman, *American Guerrilla*; William R. Peers and Dean Brelis, *Behind the Burma Road: The Story of America's Most Successful Guerilla Force* (Boston: Little Brown, 1963).

[87] Joint Staff, J-7, *Planner's Handbook for Operational Design* (Suffolk, VA: Joint Staff, 2011), http://www.au.af.mil/au/awc/awcgate/dod/opdesign_hbk.pdf.

[88] Cox, "Role of SOF;" Sacquety, "Organizational Evolution of OSS Detachment 101;" Wenner, "Detachment 101 in the CBI."

DET 101 engaged in the first phase of modern UW during this timeframe. Eifler, Peers, and the DET 101 staff accomplished tasks in this phase by establishing strong liaison relationships with CBI headquarters, OSS Washington, and British and Indian units currently operating in Burma. By building these relationships, the detachment was able to adequately tap into the intelligence and operational networks necessary to prepare the theater for the introduction and execution of UW.[89]

The detachment was able to achieve a great deal of success during the war, despite a resource constrained theater, a confusing chain of command (primarily between CBI headquarters and OSS Washington), and a complicated mission The initial long-range and short-range penetration missions enabled the detachment to identify a suitable proxy force partner in the Kachin tribesmen. Once identified and recruited, the detachment set to the task of training this proxy force at their "jungle warfare" school which was established at their headquarters in Nazira. Once trained, the Kachins operated as an ideal force for the purpose of clandestine intelligence collection. This role expanded into sabotage, subversion, and espionage operations. Guerrilla groups of Kachins also became adept at executing ambushes and other harassment operations against Japanese forces in Burma.[90]

The second phase of UW was relatively easy for DET 101 to accomplish because many exiled groups were willing to assist allied efforts against the Japanese. The detachment previously identified Kachin tribesman as the ideal partner. This enabled the transition to the third phase, infiltration of U.S. forces into enemy territory to link-up with resistance groups, which DET 101 achieved fairly easy. In fact, phase two and three happened close to simultaneously.[91]

The fourth phase of UW was primarily conducted through the training and organizing of proxy forces at their Nazira "jungle warfare" school. This school was very

---

[89] Wenner, "Detachment 101 in the CBI."

[90] Cox, "Role of SOF;" Hilsman, *American Guerrilla*; Paddock, *US Army Special Warfare*; Peers and Brelis, *Behind the Burma Road*; Wenner, "Detachment 101 in the CBI."

[91] Department of the Army, Special Forces (TC 18-01), 1-8–1-9; Wenner, "Detachment 101 in the CBI."

successful in training the Kachins in advanced communications, clandestine intelligence collection, sabotage, subversion, espionage, and tactical skills.[92] The skills gained at the Nazira facilities resulted in, the fifth phase, build-up of the capacity and capability of resistance organizations being easy.[93] From 1942 to 1945 the capacity and capability of DET 101's paramilitary forces continued to grow.

Although early failures of long range penetration operations might indicate otherwise, the unit eventually came to understand and plan for the operational reach of the Kachins. Several lines of operation also evolved through the campaign. These lines of operation ranged from early penetration and recruiting operations to the eventual use of guerrilla forces, in a conventional role, against the Japanese in the Shan States. In addition, Eifler (and later his successor William Peers) continued to evolve their forces and functions through a constant negotiation with CBI headquarters and OSS Washington. By the end of the war the unit had functioning administrative, training, operations, moral operations (predecessor to psychological operations), intelligence, and counter-intelligence sections and capabilities.[94]

During the sixth phase of UW, DET 101 successfully employed proxy guerrilla fighters until the end of the active opposition in Burma (approximately 1945). From 1942 to 1945, the detachment conducted UW operations against the Japanese in the CBI Theater. The most highly publicized operation that occurred during this period was the detachment's support to Merrill's Marauders (5307th Composite Unit, code named "Galahad") in its operation to infiltrate and seize Myitkyina. DET 101's paramilitary forces would act as guides and scouts to "Galahad." In addition, they would screen the movements of the force as it conducted its infiltration and exfiltration from the objective. Despite heavy losses, Merrill's Marauders were successful in recapturing Myitkyina from

---

92 Sacquety, "Organizational Evolution of OSS Detachment 101;" Wenner, "Detachment 101 in the CBI."

93 Department of the Army, Special Forces (TC 18-01), 1-8–1-9.

94 Sacquety, "Organizational Evolution of OSS Detachment 101."

the Japanese. This success is due, in no small part, to the contributions of DET 101 during the operation.[95]

On the other side of the spectrum, the detachment saw the least amount of success when its forces were used in a conventional role toward the end of the war. Following the success of retaking Myitkyina in support of "Galahad," the detachment received a directive to swell the ranks of its paramilitary to 10,000 guerrilla proxy forces. This led the detachment to be used in a conventional role when it was ordered to clear Japanese forces from the Shan States. Though eventually successful, DET 101's guerrilla forces would take more casualties during this operation than any other point in the campaign.[96] Shortly after operations in the Shan State, active conflict in the CBI Theater ended and the detachment transitioned to the final phase of UW by standing down their proxy and guerrilla forces.

By the end of the war, DET 101 inflicted an estimated 10,000 casualties (killed or seriously injured) on the Japanese, while only suffering several hundred of their own. Additionally, they destroyed hundreds of bridges, trains, and military vehicles through their sabotage operations. Perhaps most impressive, the detachment provided a vast majority of the actionable intelligence used in the CBI Theater. Some estimates state that over 80% of Air Force targets in the theater were selected based on intelligence provided by DET 101.[97]

2. Operations

Examining the DET 101 case study in Burma reveals that conditions in occupied China, Burma, and India provided an ideal situation for group behavior social mobilization. Social mobilization theories seek to explain why individuals establish groups and organizations for common causes. Of particular interest to this research is the

---

[95] Sacquety, "Organizational Evolution of OSS Detachment 101," 109–14; Wenner, "Detachment 101 in the CBI," 40–42.

[96] Ibid.

[97] Cox, "Role of SOF;" Hilsman, *American Guerrilla*; Paddock, *US Army Special Warfare*; Peers and Brelis, *Behind the Burma Road*; Sacquety, "Organizational Evolution of OSS Detachment 101;" Wenner, "Detachment 101 in the CBI."

"start-up problem" and what motivates individuals to move past selfish motivation and engage in collective behavior.[98]

The Japanese occupation created a social dilemma causing otherwise unconnected groups of people to band together for a common purpose.[99] Additionally, the Japanese were not benevolent occupiers. Harsh treatment of locals gave additional motivation for otherwise disconnected groups to overcome the cost of punishment (capture, torture, or even death) to band together in resistance organizations.[100] Collective action calls this cost and benefit equation as the "start-up problem," in which individuals overlook the costs (risks to life or family) for the benefits they will receive (freedom from oppressive occupiers).[101]

Conditions created by the Japanese made the job of recruiting resistance, proxy, and guerrilla forces relatively simple for DET 101 personnel. As previously stated, there were many potential groups of people in the CBI Theater that the detachment could have chosen as a partner force. Additional factors made recruitment of Kachins the ideal choice. First, they were a minority group that was subjugated by the British colonial authority prior to Japanese occupation. Second, due to colonial exploitation, they were regularly pitted against other ethnic groups in the area causing their group to be tightly knit. Third, they did not see the Americans as colonial occupiers or as an oppressive group. Finally, they were already formed into unorganized resistance groups prior to DET 101's arrival.[102] These factors made large-scale recruitment an attainable goal for DET 101.

---

98 Centola, "Homophily, Networks, and Critical Mass;" Olson, *Logic of Collective Action*; Ostrom, "Behavioral Approach;" Ostrom, "Analyzing Collective Action;" Ostrom, "Collective Action and the Evolution."

99 Ostrom, "Behavioral Approach."

100 Sacquety, "Organizational Evolution of OSS Detachment 101;" Wenner, "Detachment 101 in the CBI."

101 Centola, "Homophily, Networks, and Critical Mass;" Olson, *Logic of Collective Action*; Ostrom, "Behavioral Approach;" Ostrom, "Analyzing Collective Action;" Ostrom, "Collective Action and the Evolution."

102 Sacquety, "Organizational Evolution of OSS Detachment 101," 26–29.

Information age technologies, particularly the Internet, could make the job of recruitment even easier. First, advanced communication, offered by the Internet, could reduce the risks to DET 101 by eliminating the need to immediately conduct physical infiltration into Japanese occupied territory to identify potential resistance groups. Social media could provide a platform to interact with potential resistance and guerrilla membership. Additionally, the detachment could exploit social network analysis (SNA) tools to gain additional insights into fledgling resistance groups, including which members are more central to an organization, authority figures, and members who broker social capital (or provide connections between groups).[103]

In a state and counter-state conflict, indoctrination of resistance groups is a major factor. In this case, it was not a major concern to DET 101 forces. At the time of initial contact, the detachment found a group that was already resolutely anti-Japanese and pro-Ally.[104] Although cultural and language barriers needed to be overcome, war-time conditions provided an environment where indoctrination became a minor factor.

Even though indoctrination was not a major activity for DET 101, advanced Internet communications platforms would have provided a distinct advantage to a force wishing to proselytize a proxy group. SNA could have provided the visibility necessary to insert information through members of the network most likely to propagate material throughout the entire network.[105] Once again, this would have alleviated the need for UW practitioners to physically infiltrate areas, early in the UW operation to establish and maintain conditions necessary for the morale and desired mindset of resistance forces.

The jungle environment of Burma provided an excellent base for training and operationalizing guerrilla forces. As previously discussed, DET 101 established and operated a robust training facility at their Nazira headquarters. At the "jungle warfare"

---

[103] Everton, *Disrupting Dark Networks*; Everton, "Tracking, Destabilizing and Disrupting;" Granovetter, "Strength of Weak Ties;" Prell, *Social Network Analysis*; Roberts and Everton, "Strategies for Combating Dark Networks."

[104] Sacquety, "Organizational Evolution of OSS Detachment," 26–29.

[105] Everton, *Disrupting Dark Networks*; Everton, "Tracking, Destabilizing and Disrupting;" Granovetter, "Strength of Weak Ties;" Prell, *Social Network Analysis*; Roberts and Everton, "Strategies for Combating Dark Networks."

school, the detachment was able to train the Kachin in a wide variety of skills including communications, clandestine intelligence collection, sabotage, and advanced guerrilla tactics. Although forward based were established (Operation "Forward" and "Knothead"), the Nazira base also afforded the detachment an ideal location from which to launch operations resistance forces.[106]

Training of UW forces is difficult to conduct or enhance in a digital or Internet environment. Although it is difficult, it is not entirely impossible. UW practitioners can learn lessons by studying terrorist organizations. Terrorists use the Internet to post materials giving detailed instructions on subjects ranging from how to build bombs to kidnapping Americans. Capitalizing on even more advanced technologies, the terrorist-affiliated organization Hizballah designed and disseminated a video game giving players the ability to conduct missions against Israeli soldiers.[107] Advances in virtual reality (VR) training and the decreasing costs of VR hardware can also potentially be exploited in future UW scenarios.[108]

Training forces in the digital environment is a fairly new requirement. Information and cyber technologies could have enhanced DET 101's Moral Operations (psychological operations) and also allowed them to attack enemy communications and other critical infrastructures. Inevitably, operationalization of forces is the UW activity where the barrier between the digital and physical world must be breeched. Cyber-enabled operations have the potential to remove that barrier, therefore reducing the risks that must be taken by UW operators.

---

[106] Hilsman, *American Guerrilla*; Sacquety, "Organizational Evolution of OSS Detachment 101;" Wenner, "Detachment 101 in the CBI."

[107] Jarret Brachman and James J.F. Forest, "Exploring the Role of Virtual Camps," in *Denial of Sanctuary: Understanding Terrorist Safe Havens*, ed. Michael Innes (Westport, CT: Praeger, 2007), 124–48.

[108] Loren Bymer, "Virtual Reality Used to Train Soldiers in New Training Simulator," *Army.mil*, August 1, 2012, http://www.army.mil/article/84453/; Brian Shuster, "Could Virtual Reality Revitalize the Economy?" *Wired*, October 2014, http://www.wired.com/2014/10/virtual-reality-economy/.

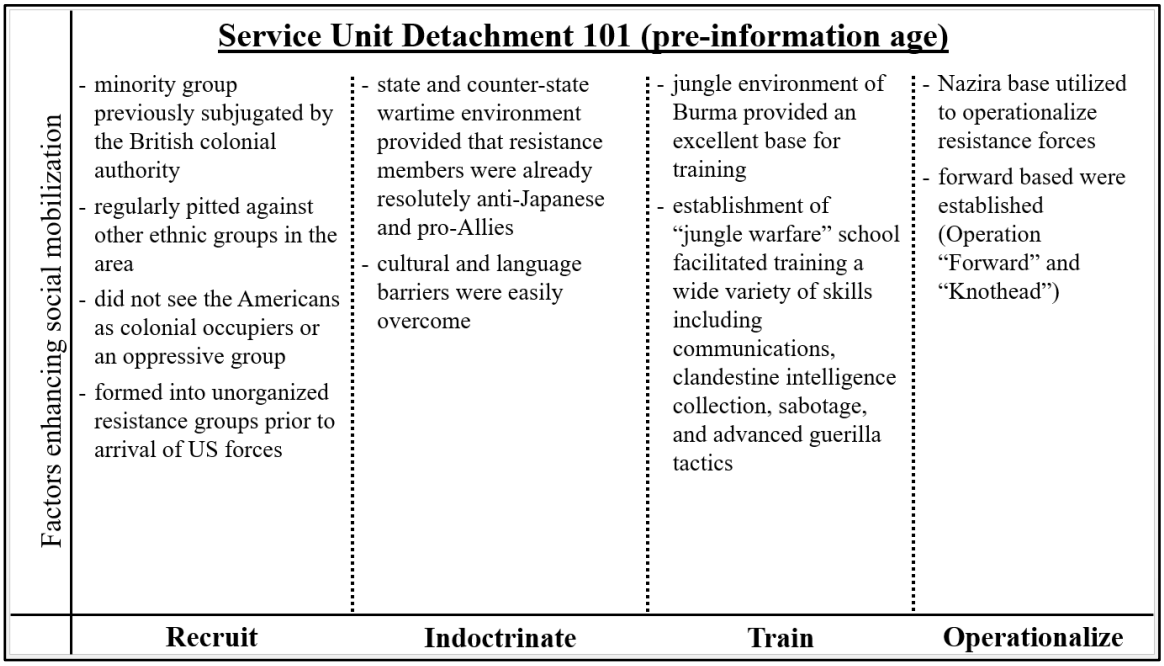
3. Summary

This case study provides an excellent example of how successful UW can produce strategic effects in war. Many factors including leadership of the unit; organizing and training of DET 101 personnel; and factors in the operational environment led to the successful recruitment, indoctrination, training, and operationalizing of competent and effective guerrilla forces. Through examination of U.S. doctrine for UW, it is clear that current techniques and procedures are a direct reflection of this historical case. As such, this example reflects the seven phases of contemporary U.S. doctrine for UW.

DET 101 also exploited conditions in the operational environment that were conducive to social mobilization. The "start-up problem" was easily overcome, creating an ideal environment for the initial recruitment and indoctrination of indigenous personnel. It is evident that information age technologies, particularly those provided through SNA tools could have facilitated activities in the four areas examined: recruitment, indoctrination, training, and operationalizing resistance and guerrilla forces. This case study will be the only one examined in the pre-information age environment.

Conditions that enhanced Detachment 101's social mobilization during the UW operation in Burma that fall within the four areas of activity are highlighted in the analysis framework shown in Figure 4.

Figure 4. Service Unit Detachment 101 Analysis



B. RUSSIA VERSUS GEORGIA: THE SOUTH OSSETIA CAMPAIGN

The Cold War ended in 1991. To the relief of many, this happened not with the flash of nuclear Armageddon, but instead with a drastic shift in the policy of the Soviet Union under Mikhail Gorbachev. This transformation from a tense bi-polar world to a multi-polar one (with only a single-super power remaining), ushered in a new era, particularly for countries in Eastern Europe. This new system allowed the small Republic of Georgia to break away from their former host country.[109]

Following the collapse of the United Soviet Socialist Republic (U.S.S.R.), U.S. diplomatic, intelligence, and military agencies changed their focus from Communism, and the threat of World War III, to the growing threat of terrorism. Along these same lines, the hub of the U.S. intelligence apparatus (the Central Intelligence Agency or CIA), under the George H.W. Bush administration, reorganized its efforts to combat

[109] Richard Ned Lebow and Thomas Risse-Kappen, *International Relations Theory and the End of the Cold War* (New York: Columbia Univ. Press, 1996), 9–11, http://nuesaui2014.com/ebooks/political%20 science/International%20relation%20Theory.pdf.

"transnational issues" including terrorism, drugs, the proliferation of weapons of mass destruction, and crime.[110] The terrorist attacks against the U.S. on September 11, 2001 validated these new lines of operation.

After 9/11, the Russians also acknowledged terrorism to be of chief concern. With this common enemy, an unlikely partnership between U.S. and Russian political and intelligence agencies emerged.[111] This new "friendly" relationship between former rivals from East and West, made Russian military aggression against Georgia (a North Atlantic Treaty Organization (NATO) applicant country) in 2008 seem unlikely. On the contrary, the war between Russia and Georgia was the product of a deliberate policy of overt and covert actions to destabilize and eventually retake former Russian diaspora regions in Georgia.[112] Although the United States was not directly involved in this conflict, there is much U.S. UW and intelligence professionals can learn from Russia's success, particularly the use of covert cyber operations to enable both conventional and special operations forces.

This section asserts that Russia used the Georgian conflict to test new cyber-enabled UW, cyber-attack, and cyber-propaganda, to support the deployment of its conventional military forces. To reach this conclusion, the first sub-section discusses Russian political, military, and intelligence doctrine. This sub-section also presents a history of the 2008 conflict between Russia and Georgia. The second sub-section analyzes the UW activities (recruiting, indoctrinating, training, and operationalizing proxy forces) and how Russian forces used aspects of social mobilization in support of their campaign in South Ossetia. This sub-section also explores how Information Age technologies enhanced Russian operations. The final sub-section summarizes and presents a framework analysis summary of the case-study.

---

[110] William C. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington, KY: Univ. Press of Kentucky, 2006), 214.

[111] Angela Stent and Lilia Shevtsova, "America, Russia and Europe: A Realignment?" *Survival* 44, no. 4 (2002): 121–34, doi: 10.1080/00396330212331343532.

[112] "The Russo-Georgian War 2008: The Role of Cyber Attacks in the Conflict," Armed Forces Communications and Electronics Association (AFCEA), May 24, 2012, 2–5, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

1. Background

This section will be split into two parts. The first part will explain Russian information, intelligence, and warfare doctrine. The second section will describe the 2009 conflict between Russia and Georgia over South Ossetia.

a. The Evolution of Russian Warfare

Russia recognizes that information warfare is crucial for destabilizing the West and regaining control of the ethnically Russian Diasporas.[113] *Spetspropaganda* (special propaganda) was re-introduced in 2000, and has since been taught to specialists in Russian military and intelligence services. Of particular interest, Russian information warfare doctrine includes and integrates cyber techniques into special propaganda.[114]

To further emphasize this key factor, top Russian military leader, Valery Gerasimov, authored an article titled "The New Generation Warfare," which documents Russia's intent of destabilizing and manipulating countries in the information space prior to the incursion of special operations or conventional military forces. This article lays out Russian military and intelligence doctrine and how it relies on digital and information technologies to execute covert and clandestine information programs to influence targeted populations (government, military, and civilian).[115] Current Russian strategy was developed using old Soviet ideas and tested on modern battlefields.

Digital information and cyber warfare techniques were successfully tested, on a limited scale, in Estonia in 2007. One year later, during the South Ossetia conflict, Russia

---

[113] Darczewska, "Anatomy of Russian Information Warfare."

[114] Ibid.

[115] Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *World Post*, February 9, 2014, http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html; Gerasimov, "New Generation Warfare." Original Gerasimov doctrine is a Russian Language document that was translated using google docs. In addition, the link to this document may contain viruses, reader is to access at their own risk. Coalson's article provides a synopsis and translation of portions of the original article.

was much more successful in the cyber realm by combining cyber activities in support of overt military actions.[116]

b. Russia versus Georgia: Cyber Proxy War

The tension between Russia and Georgia over the South Ossetia region did not start in 2008. The two countries had been in a state of low level conflict, which has often resulted in violence between opposing ethnic groups since the early twentieth century. After the collapse of the U.S.S.R., the ethnically Russian regions of South Ossetia and Abkhazia demanded sovereignty from the Georgian government. To add to this problem, and to begin setting the stage for future action, Russia exploited these minority regions by offering Russian citizenship to any person who resided in a previously Soviet controlled area. In this way they were able to intervene into the affairs of these countries under the auspices of aiding their citizens.[117]

The issue of re-integrating breakaway regions continued through the 1990s and well into the first decade of the new millennium.[118] The eventual conflict in 2008 was set into motion following "[the] Rose Revolution of November 2003, together with the subsequent election of Mikhail Saakasvilli in 2004, [reigniting] Georgian nationalist sentiment."[119] The Saakasvilli government pursued a campaign to re-integrate the South Ossetia and Abkhazia regions. Relations between the Russian Federation and Georgia deteriorated even more after NATO officially recognized Kosovo in 2008 and Georgia continued to pursue NATO membership.[120]

The conflict officially began on August 8, 2008, when Russian forces crossed the border into South Ossetia. Although Russia asserted that the movement of troops was to reinforce their peace keeping operation in the area, the Georgian Government saw this aggression as reason to declare war and began shelling the South Ossetia capital of

---

[116] Thomas, "Bear Went Through the Mountain," 31–67.

[117] AFCEA, "Russo-Georgian War 2008," 2–3.

[118] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace," 7–8.

[119] Ibid., 7.

[120] Ibid., 7–8.

Tskhinvalli.[121] Russia deployed naval, air, and ground forces to participate in the conflict. The more heavily equipped Russian forces, in support of South Ossetia militia, were able to defeat the lighter armed Georgian troops.

Despite the long and deeply rooted disagreements that fueled this conflict, major combat operations were not spectacular and the war only lasted for five days. Arguably, the more interesting part of this contest happened on the cyber battlefield and originated from servers and computers located within Russian sovereign territory.[122] The Georgian government started to recognize cyber-attacks several weeks before the deployment of Russian forces. The volume, sophistication, and intensity of cyber-based operations continued to increase through the end of the conflict. These attacks targeted government, media, and economic sites, negatively affecting the Georgian government's ability to communicate with its population at a time of crisis and uncertainty.[123]

Russian hackers achieved this effect by using a relatively simple technique known as a distributed denial of service (DDoS) attack. By pushing too much data to a computer, site, or server, these types of attacks effectively prevent "legitimate" users from accessing information technology resources.[124] The DDoS attacks were so effective in limiting the Georgian government's ability to communicate through Internet resources, it forced them to relocate critical servers to locations outside of the country (particularly in the United States and Estonia).[125]

In addition to DDoS attacks, Russian hackers also conducted cyber-propaganda operations intended to sway local Georgian and international opinion. Hackers disseminated web-propaganda through "[Structured Query Language (SQL)] [injections], which [use] a test field on a webpage to directly communicate with the back end database (normally, a common SQL database—hence the name)."[126] The most commonly cited of

---

[121] Ibid.

[122] Hollis, "Cyberwar Case Study."

[123] AFCEA, "Russo-Georgian War 2008," 7–8.

[124] Shakarian, "2008 Russian Cyber Campaign," 63–64.

[125] Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace," 11.

[126] Shakarian, "2008 Russian Cyber Campaign," 64.

these propaganda attacks was when the website of the Georgian government was defaced and embedded with an image comparing President Saakashvili to Hitler.[127]

In the conflict with Georgia, Russia categorically denies involvement in the cyber domain. Instead they assert that the actions were organized and executed by patriotic citizens (most likely Russian government proxies). A Russian military official even reversed the blame stating that the attacks were "a response to Georgians hacking South Ossetia media sites earlier in the week."[128] This demonstrated act of plausible deniability is the first aspect that lends credence to the assertion that Russian political, military, and intelligence services helped to orchestrate cyber-enabled operations in the South Ossetia conflict.

Despite Russia's denial of their involvement, the Georgian government and multiple international journalists assert that Russians were responsible for cyber operations during the war.[129] Several reasons are given for making this connection. First, the timing of the cyber-attacks, particularly the DDoS attacks, were said to have been synchronized too well with the introduction of conventional military forces to have happened by chance. This suggested that the parties responsible at least received information and possibly instructions from elements in the Russian government and intelligence services. Second, the key government, economic, and infrastructure sites targeted in cyberspace were not the same as the targets of Russian ground troops. This suggested that the Russian military understood the effects that cyber-attacks would have and did not waste resources in a duplication of efforts.[130]

---

[127] Ibid.

[128] Shakarian, "2008 Russian Cyber Campaign," 64.

[129] Ward Carroll, "Cyber War 2.0 — Russia v. Georgia," *Defense Tech*, August 13, 2008, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/; Kim Hart, "Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar," *Washington Post*, August 14, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html; Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html; John Leyden, "Bear Prints Found on Georgian Cyber-attacks," *Register*, August 14, 2008, http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/; John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&.

[130] Carroll, "Cyber War 2.0;" Hart, "Longtime Battle Lines;" Krebs, "Report: Russian Hacker;" Leyden, "Bear Prints Found;" Markoff, "Before the Gunfire."

2. Operations

The 2008 conflict between Georgia and Russia provides an example where factors in the operational environment provided conditions for the synthesis of group behavior or social mobilization.[131] Russian forces exploited factors in the environment to lower the costs of participating in this proxy-cyber network. This helped with the initial tasks of recruiting and indoctrinating a cyber-enabled counter-state network.

First, it is important to re-emphasize that the majority of South Ossetia citizens are ethnically similar and consider themselves to be a part of the Russian diaspora.[132] Inherent to the tasks of recruiting and indoctrinating cyber-proxy forces is Russia's belief that "information battles are necessary for the Russian and Eurasian civilization to counteract informational aggression from the Atlantic civilization led by the USA."[133] This belief is derived from Russian academic, political, and military doctrine. These convictions are indoctrinated into all members of the Russian-speaking diaspora from a young age through state controlled media outlets. From this position, the legitimate annexation of all of the culturally Russian diaspora regions is seen as a patriotic duty.[134]

The digital environment, in which the Russian cyber proxy forces operate, also reduces barriers that may otherwise inhibit potential members from joining during a turbulent crisis in South Ossetia. These key factors include a low cost of entry, sparse regulations by national and international organizations, anonymity and secrecy provided to members, the speed of information, and a wide variety of available multimedia.[135]

Training and operationalizing forces for the cyber-battlefield did not fall directly on the shoulders of Russian military or political leaders. According to Franke Ulrik's extensive report on Russian non-kinetic tactics, Moscow feels that plausible deniability of

---

[131] Centola, "Homophily, Networks, and Critical Mass," 3–40; Olson, *Logic of Collective Action*; Ostrom, "Behavioral Approach;" Ostrom, "Analyzing Collective Action," 155–66; Ostrom, "Collective Action and the Evolution," 235–52.

[132] Darczewska, "Anatomy of Russian Information Warfare."

[133] Ibid., 5.

[134] Ibid.

[135] Weimann, "How Modern Terrorism Uses the Internet."

covert cyber campaigns is desirable. This leads Russian agents to use proxies and "go-betweens" to facilitate operations on the cyber battlefield.[136] Exactly how this was accomplished in the Ossetia campaign, and by what proxies, has not been publically acknowledged by the Russian government, but the use of these techniques are called for in Russian political and military doctrine.[137]

One proxy that was used is the Russian Business Network (RBN). The RBN is an organized criminal group that claimed a degree of responsibility for cyber-operations during the 2008 conflict. The RBN helped organize and recruit hackers for this effort and additionally supplied advanced software and hacking techniques to these so-called "cyber militias."[138] This lends further credence to the theory that the cyber portion of this campaign was a covert UW-like effort.

It is also reasonable to assert that the Russian government recruited, synchronized, and operationalized these proxy forces to support its military objectives. The use of proxy forces also allowed the Russian Federation to continue denial of these actions despite what some journalists and scholars assert is irrefutable evidence to the contrary.[139]

These factors significantly lowered the risks associated with social mobilization and allowed Russian forces to recruit, indoctrinate, train, and operationalize a proxy cyber force that enhanced the results obtained by their conventional and special operations forces. Additionally, Information Age technologies, principally the Internet, made the job of recruiting even easier. Advanced communication, offered by the Internet, reduced the risks to Russian agents by eliminating the need to conduct an immediate

---

[136] Ulrik Franke, "War by Non-Military Means: Understanding Russian Information Warfare," Swedish Defence Research Agency, 2015, http://www.foi.se/ReportFiles/foir_4065.pdf.

[137] Darczewska, "Anatomy of Russian Information Warfare;" Franke, "War by Non-Military Means."

[138] Jeremy Kirk, "Georgia Cyberattacks Linked to Russian Organized Crime," *Computerworld*, August 17, 2009, http://www.computerworld.com/article/2527019/government-it/georgia-cyberattacks-linked-to-russian-organized-crime.html; Joseph Menn, "Expert: Cyber-Attacks on Georgia Websites Tied to Mob, Russian Government," *Los Angeles Times*, August 13, 2008, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

[139] Carroll, "Cyber War 2.0;" Hart, "Longtime Battle Lines;" Krebs, "Report: Russian Hacker;" Leyden, "Bear Prints Found;" Markoff, "Before the Gunfire."

physical infiltration into South Ossetia. This also provided an additional layer between the Russian government and their proxy cyber force. This separation helped Moscow to maintain plausible deniability with regard to their operations in the cyber domain.

Although there is no direct evidence that Russia used Social Network Analysis (SNA) in the conflict with Georgia, SNA software could have been used to gain insights into potential proxy forces. These insights include which members are more central to an organization, which are authority figures, and which bridge social capital (or provide connections between groups).[140] The use of SNA could also provide the visibility necessary to insert information through members most likely to propagate material throughout the entire network.[141] Once again, this would alleviate the need for Russian government agents to physically infiltrate (early in the operation) to establish and maintain conditions necessary for the morale and desired mindset of proxy forces.

Training of proxy forces is difficult in a digital or Internet environment. During this crisis, the RBN and Russian "hacking" forums provided information on advanced cyber warfare techniques. Additionally, Russian information warfare doctrine stresses the need to integrate cyber and physical warfare. It also encourages the use of digital technologies in modern operations.[142] Although not seen in this conflict, the decreasing costs of virtual reality hardware will inevitably become a tool for the training of future digital warriors.[143]

Operationalizing forces in the digital environment is a fairly new occurrence. Information age technologies enhanced Russian *spetspropaganda* (psychological and deception operations) and cyber-attack capabilities in the digital environment, allowing them to attack enemy communications and other critical infrastructures. Inevitably,

---

[140] Everton, *Disrupting Dark Networks*; Everton, "Tracking, Destabilizing and Disrupting;" Granovetter, "Strength of Weak Ties," 1360–80; Prell, *Social Network Analysis*; Roberts and Everton, "Strategies for Combating Dark Networks."

[141] Everton, *Disrupting Dark Networks*; Everton, "Tracking, Destabilizing and Disrupting;" Granovetter, "Strength of Weak Ties," 1360–80; Prell, *Social Network Analysis*; Roberts and Everton, "Strategies for Combating Dark Networks."

[142] Kirk, "Georgia Cyberattacks Linked;" Krebs, "Report: Russian Hacker."

[143] Loren Bymer, "Virtual Reality Used to Train;" Brian Shuster, "Could Virtual Reality Revitalize?"

operationalization of forces is the activity where the barrier between the digital and physical world must be breached. These cyber-enabled unconventional operations potentially moved that barrier to the digital side, therefore reducing the risks that had to be taken by Russian military and intelligence service agents.

3. Summary

The campaign in cyberspace against Georgia was used to destabilize and influence the physical environment in an UW-like fashion. Since this campaign was executed by proxy forces, Russian authorities have been able to continue to deny involvement. This denial and use of proxies provides credibility to the theory that cyber-attacks and cyber propaganda were a deliberate unconventional operation. Although it is unlikely that the Russian government will disclose its involvement in these cyber-attacks anytime in the near future, it is clear that Russian intelligence and military leadership used lessons learned during their 2008 incursion in Georgia to develop their current Information Warfare doctrine.[144]

In the future, Russia may continue incursions into the sovereign territory of other state actors to support the ethnically Russian diaspora. The Georgian case study shows that, even seven years ago, Russia was developing and building refined covert information warfare capability and capacity to enhance their ability to recruit, indoctrinate, train, and operationalize proxy forces. Their new military and political doctrine confirms that these cyber techniques will continue to be a factor in how they achieve their national strategic goals. Lessons from this case study, including how proxy cyber forces influenced and set conditions for conventional and special operations, have the potential to be applied when rethinking future U.S. UW doctrine.

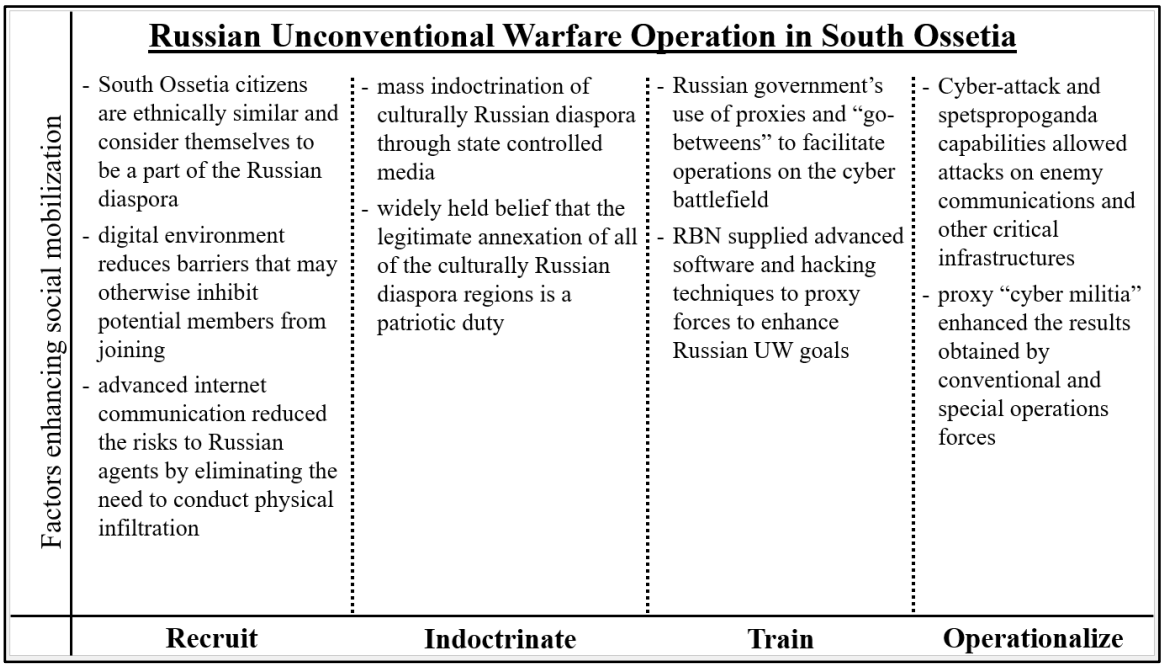
In the 2008 conflict, Russia achieved many of its goals. It also learned valuable lessons for use in its future campaigns. U.S. policy makers and UW professionals can gain valuable insights from analysis of the techniques used in the cyber-portion of this

[144] Keir Giles, "'Information Troops,'" 1–16.

conflict. Capitalizing on these successful methods to structure U.S. understanding of cyber-enabled UW will open up new low-cost, low-footprint options for future conflicts.

The factors that enhanced Russia's social mobilization during the unconventional warfare operation in South Ossetia that fall within the four areas of activity are highlighted in Figure 5.

Figure 5. South Ossetia Analysis.



C. RUSSIA VERSUS UKRAINE: THE CRIMEA ANNEXATION

This case study is relevant because it represents a recent use of UW by a state actor, Russia. The UW operation was a stunning success and showed a dramatic capability increase when compared to their 2008 operation in South Ossetia. As was demonstrated in the South Ossetia Campaign, the conditions for social mobilization were ideal and Russia exploited these same conditions with the Crimea annexation. This case study will identify how Russia conducted a UW operation by blending real world paramilitary operations with cyber-enabled capabilities, resulting in the annexation of Crimea. The case study will start with a brief history of Crimea followed by the events

leading up to Russia's UW operation. Next, the case study will focus on Russia's UW operation, broken down into five broad topic categories: paramilitary operations, cyber warfare, deception, propaganda, and policy. The case study will then describe the social mobilization factors that led to Russia's successful UW operation in regard to the selected categories of recruitment, indoctrination, training and operations.

Over the course of approximately a month between February and March 2014, Russia annexed sovereign Ukrainian territory and stirred fears of a new Cold War. In early February 2014, with the pro-Russian Ukrainian government losing control and falling later that month, Russia planned and executed an unconventional warfare operation to annex Crimea.[145] Paramount to the success of this operation was Russia's use of cyberspace operations during the entire spectrum of the UW operation.

1. Background

The background of this case will be broken into two parts. The first part will describe the historical background of Russia's relationship with the Crimean region. The second part will describe the events that led to the annexation of the Crimea by the Russian Federation.

a. Crimea's Russian History

Crimea has a long historical affiliation with Russia dating back to the late 1700s when it was first annexed by the Russian empire for its port at Sevastopol.[146] During the reign of the Soviet Union, the control of Crimea was transferred to Ukraine by then First Secretary of the Communist Party Nikita Khrushchev and was the homeport of the Black Sea Fleet (currently territory of the U.S.S.R.).[147] With the collapse of the Soviet Union, Ukraine became independent in 1991 and Crimea was recognized as an autonomous

[145] Emmanuel Karagiannis, "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals," *Contemporary Security Policy* 35, no. 3 (September 2014): 400–20, doi: 10.1080/13523260.2014.963965; Jeff Seldin, "Report: Kremlin Was Eying Ukraine Prior to Yanukovych Ouster," *Voice of America*, February 24, 2015, http://www.voanews.com/content/russia-ukraine-novaya-gazeta-strategic-document/2657107.html.

[146] Karagiannis, "Russian Interventions in South Ossetia," 400–20.

[147] Ibid.

republic inside Ukraine with a majority of Crimeans identifying themselves as Russian.[148] In 1997, the Partition Treaty signed between Russia and Ukraine split the Black Sea Fleet with 81.7% of the vessels going to Russia and allowing Russia long-term use of the navy port facilities in Sevastopol.[149]

b. The Events Leading to Russia's Unconventional Operation

Ukraine has historically fallen within the Russian sphere of influence and more recently within Russia's "near abroad." It occupies a strategic position between the European Union and NATO member states on one side and Russia with its Black Sea Fleet based in Crimea on the other. Since the end of the Cold War both sides have attempted to influence Ukraine to join their respective spheres of influence and it appeared Ukraine was leaning towards the west until November 2013.

At the last-minute in November 2013, Ukrainian President Yanukovych decided to scrap an economic trade deal with the European Union because of pressure from the Russian government.[150] Massive anti-government protests broke out in Kiev, the capital of Ukraine, that lasted for three months alternating between violent and peaceful actions. On February 18, 2013, by the orders of President Yanukovych, elite Ukrainian riot police known as "Berkut" broke the protest through the use of deadly force, using snipers and hired government thugs, resulting in the death of over 100 people and hundreds more injured.[151] Over the next few days the Parliament acted, disbanding the Berkut, ordering police and military forces back to their bases and causing President Yanukovych and his top officials to flee the country to Russia as they were branded wanted criminals.[152]

---

148 Karagiannis, "Russian Interventions in South Ossetia," 400–20.

149 Ibid.

150 Steven Woehrel, *Ukraine: Current Issues and U.S. Policy* (CRS Report No. RL33460) (Washington, DC: Congressional Research Service, 2011), http://fpc.state.gov/documents/organization/164374.pdf.

151 Ibid.

152 Ibid.

Protesters seized key government buildings in Kiev and on February 27, a new pro-Western government was formed by the Ukrainian Parliament.[153]

2. Operations

Russian intelligence activities and preparations for UW within Crimea appear to have begun early during the crisis in Kiev. This involvement was due to Crimea's strategic position, historical ties, and status as home to Russia's Black Sea Fleet, which hosts approximately 11,000 Russian navy and support personnel. Russian intelligence services "thoroughly penetrated" the Ukrainian military, police, and intelligence services.[154] Additionally, according to Langton, Director of Independent Conflict Research and Analysis in London, Russia conducted extensive work prior to the conflict by training and organizing "small local units among Crimea's ethnic Russians that could be activated in times of tension."[155]

With the world's attention focused on the Winter Olympics in Sochi, the Russian government quietly increased its UW activities in Crimea. By early February 2014, mass rallies were organized in Crimea by pro-Russian political parties, which included a protest in Sevastopol of 50,000 people.[156] During this time Russian entities in Crimea started "recruiting local self-defense forces" from the organized rallies, with the recruitment numbering upwards of 10,000 individuals.[157] These conditions allowed Russia to establish the mobilization structures required within collective action that directly assisted with the UW operation.

---

153 Ibid.

154 Woehrel, *Ukraine: Current Issues*, 3.

155 Ron Synovitz, "Russian Forces in Crimea: Who Are They and Where Did They Come From?" *Radio Free Europe/Radio Liberty*, March 4, 2014, http://www.rferl.org/content/russian-forces-in-crimea--who-are-they-and-where-did-they-come-from/25285238.html.

156 Maksym Bugriy, "The Crimean Operation: Russian Force and Tactics," *Eurasia Daily Monitor* 11, no. 61, April 1, 2014, http://www.jamestown.org/regions/europe/single%20/?tx_ttnews%5Bpointer%5D=6&tx_ttnews%5Btt_news%5D=42164&tx_ttnews%5BbackPid%5D=51&cHash=fc393270652afcca3fe0563fcc63c5a0#.VVS9nZNyznd.

157 Ibid.

a. Paramilitary Operations

The main thrust of Russia's UW operation took place within the area of paramilitary operations after the pro-Russian Ukrainian President Yanukovych fled and the Ukrainian Parliament appeared to pivot away from Russia and toward the West. Paramilitary operations involve using some sort of unconventional or special operations force to conduct actions that may require the "use of force" or to train individuals to conduct such operations.[158]

On February 26, 2014, elite Russian Special Forces, GRU Spetsnaz commandos (from the Main Intelligence Directorate of the General Staff of the Armed Forces), and airborne unit personnel deployed to Crimea via Black Sea Fleet vessels and Mi-24 helicopters. Russia essentially moved a Trojan Horse into Crimea through their ports.[159] This paramilitary force wore brand new green uniforms, black ski masks, and no rank or insignia; they were dubbed the "little green men."[160] The Russian paramilitary force surrounded key Ukrainian government facilities in Crimea, including military bases containing 18,000 Ukrainian military personnel, airports and local Crimean government buildings.[161] The Russian navy also participated forming a blockade of Crimea in the Black Sea, which prevented Ukraine's navy from reacting to the events in Crimea.[162]

Over the next few days, Russian forces seized "control of Crimea's airspace, its ports, its highways, its television stations, and is regional government."[163] Russia seized an eastern Crimea port across from the Russian Kuban region and began moving

---

158 Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence* (New Brunswick, NJ: Transaction, 1995), 3.

159 Maksym Burgriy, "The Crimean Operation: Russian Force and Tactics." *Eurasia Daily Monitor* 11, no. 61, April 1, 2014; Michael Weiss, "Russia Stages a Coup in Crimea," *Daily Beast*, March 1, 2014, http://www.thedailybeast.com/articles/2014/03/01/so-russia-invaded-crimea.html.

160 Burgriy, "Crimean Operation."

161 Fred Weir, "Russia Debuts New, Sleek Force in Crimea, Rattling NATO," *Christian Science Monitor*, April 3, 2014, http://www.csmonitor.com/World/Europe/2014/0403/Russia-debuts-new-sleek-force-in-Crimea-rattling-NATO.

162 Karagiannis, "Russian Interventions in South Ossetia," 400–20.

163 Weiss, "Russia Stages a Coup in Crimea," 1.

paramilitary forces and vehicles by ferry across the strait.[164] Russia deployed a total of approximately 6,000 to 7,000 "little green men" by ship and air into Crimea.[165] Within the paramilitary force, the Russian government employed the use of private Russian security firm personnel. These individuals seized the Crimean Parliament building, the Verkhovna Rada, and wore a distinctively different military type uniform.[166] The paramilitary forces specifically targeted and seized local police stations and other government buildings that had weapons and ammunition supplies so they could be turned over to local Russian-backed forces.[167]

Unarmed Crimeans even "helped the Russian forces by surrounding Ukrainian military bases…making it very difficult for Ukrainian troops to even think about opening fire" or attempt to use force to resist the Russian actions.[168] The Russian paramilitary forces did not encounter any resistance from the Ukrainian military and security personnel and seized Crimea without firing a shot.

b. Cyber Warfare

As its paramilitary forces entered Crimea, Russia used cyber warfare to jam cell phone and Internet communications in order to knock off-line and sever the Ukrainian military command and control between units stationed in Crimea and their headquarters in Kiev.[169] "Massive denial-of-service attack[s]" were conducted against Ukrainian military and security services, which knocked out their Internet servers, severing their command and control capabilities.[170] The Ukrainian state-owned telecommunications company Ukrtelecom, which provided Internet and phone service to Crimea, reported their telecommunications infrastructure in Crimea had been degraded and they were

164 Synovitz, "Russian Forces in Crimea?"

165 Ibid.

166 Synovitz, "Russian Forces in Crimea?"

167 Gordon, "Russia Displays a New Military."

168 Weir, "Russia Debuts New, Sleek Force."

169 Gordon, "Russia Displays a New Military."

170 Russell Brandom, "Cyberattacks Spiked as Russia Annexed Crimea," *Verge*, May 29, 2014, http://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea.

unable to restore service.[171] The InfoSec Institute released a report further detailing the Russian use of cyber warfare to isolate Crimea from the rest of Ukraine and specifically discussed how multiple Crimean government websites were shut down during the UW operation.[172]

c. Deception Operations

Russia executed a series of successful deception operations within the first few days of the UW operation, though they were only thinly veiled as the action progressed. These operations were undertaken to present a false reality to a specific audience through manipulation and distortion.[173]

To dissuade Ukraine and any other country or alliance such as NATO from interfering with the Russian UW operation, Russian Defense Minister Sergei Shoigu announced a surprise military exercise consisting of 150,000 Russian troops with 40,000 of them on the border with Ukraine.[174] Under the guise of protecting Russian Black Sea Fleet personnel, the Russian Foreign Ministry informed the Ukrainian government and posted on its website that it was moving Black Sea Fleet troops between its bases in Crimea using armored personnel carriers and helicopters all "in full accordance with the foundation Russian-Ukrainian agreement on the Black Sea Fleet."[175] Additionally, throughout the UW operation President Putin continuously denied any Russian forces were involved and on March 4, 2014, stated the movement of Russian troops throughout Crimea were only involved with the "protection of our [Black Sea Fleet] installations"

---

171 Shane Harris, "Hack Attack: Russia's First Targets in Ukraine: Its Cell Phones and Internet Lines," *Foreign Policy*, March 3, 2014, http://foreignpolicy.com/2014/03/03/hack-attack/.

172 Pierluigi Paganini, "Crimea – The Russian Cyber Strategy to Hit Ukraine," *InfoSec Institute*, March 11, 2014, http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.

173 Daugherty, *Executive Secrets*.

174 Weiss, "Russia Stages a Coup in Crimea;" Gordon, "Russia Displays a New Military."

175 Weiss, "Russia Stages a Coup in Crimea."

even as the evidence mounted to show otherwise.[176] In reality, the Russians used President Putin's denials, the exercise and the guise of protecting its Black Sea Fleet personnel to move paramilitary forces into Crimea.

d. Propaganda

As soon as the UW operation began, Russian news and media outlets were employed to push the narrative that Russia needed to intervene "to rescue the Russian-speaking population from right-wing extremists and chaos" targeting both the Russian domestic and larger international audiences with the multilingual Russia Today (RT) news channel leading the charge.[177]

The Russian propaganda operation also created online "troll armies" to leverage social networks, via social media platforms, consisting of individuals and at least one company.[178] These "trolls" were paid to manage numerous fake user profiles and accounts, to tweet, post, and blog simple pro-Russian stories and opinions approximately 50 times a day.[179] The use of social media platforms by "troll armies" and other entities assisted within the conditions required of social mobilization because it significantly decreased the cost of participation and risk by those actors.

In a carefully planned announcement made via Facebook to look like a reaction to spontaneous unfolding events, the Consul General of the Russian Federation in Simferopol "began handing out Russian passports to soldiers of the Berkut detachment," the notorious riot police that had been disbanded by the Ukrainian government for shooting protesters in Kiev, under the pretense of the need to protect the Russian-speaking population.[180] At the same time, the Crimean Parliament which was under the

---

176 Roy Allison, "Russian 'Deniable' Intervention in Ukraine: How and Why Russia Broke the Rules," *International Affairs* 90, no. 6 (November 2014): 1255–97, doi: 10.1111/1468-2346.12170; Vladimir Socor, "Crimea: From Russian Putsch to Military Invasion and Possible Occupation," *Eurasia Daily Monitor* 11, no. 41, March 4, 2014, http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=42036&cHash=d022abf71c498ee019b60572d6593ea1#.VVTAUZNyznd.

177 Gordon, "Russia Displays a New Military."

178 Sindelar, "Inside Russia's Disinformation Campaign."

179 Ibid.

180 Weiss, "Russia Stages a Coup in Crimea," 5.

control of the Russian paramilitary forces "announced the formation of a Crimean Berkut special division to protect public order" as a way to legitimize the UW paramilitary force.[181]

e. Overt Policy

Throughout the UW operation in Crimea, although President Putin denied Russian involvement, Putin and his government continued to make statements asserting Russia's rights as they pertained to Crimea. Some of these included Russia's right to protect its Black Sea Fleet personnel and property, protect the Russian-speaking population and Russian citizens of Crimea from violence as is stated in the Russian Constitution, and that a humanitarian crisis was at its border.[182]

On March 1, 2014, with the world still trying to figure out who the "little green men" were, President Putin made a request to the Russian Parliament for "the use of the Armed Forces of the Russian Federation on the territory of Ukraine for the normalization of the political situation in this country."[183] The Russian Parliament approved it. By mid-March 2014, Crimean residents held a referendum to secede from Ukraine with "97% of voters back[ing] a proposal to join Russia," according to *The Washington Post*.[184] On March 18, 2014, President Putin signed a treaty officially annexing Crimea and in April, President Putin admitted that Russian military forces were involved with the UW operation in Crimea.[185]

3. Summary

Russia combined both physical and virtual UW operations, resulting in a stunning success. While the world was attempting to figure out who the "little green men" were,

---

[181] Ibid.

[182] Allison, "Russian 'deniable' Intervention in Ukraine."

[183] Weiss, "Russia Stages a Coup in Crimea."

[184] "Timeline: Key Events in Ukraine's Ongoing Crisis," *Washington Post*, May 12, 2014, http://www.washingtonpost.com/world/europe/timeline-key-events-in-ukraines-ongoing-crisis/2014/05/07/a15b84e6-d604-11e3-8a78-8fe50322a72c_story.html.

[185] Allison, "Russian 'deniable' Intervention in Ukraine."

Russia annexed the territory of another country without firing a shot. Russia's successful UW operation redrew the maps of Europe bringing Crimea within Russia's sphere of influence.

Several underlying social mobilization factors assisted Russia in their successful annexation of Crimea. First and foremost was the shared common history between Crimea and Russia and the fact that a majority of Crimeans self-identified as Russians immediately prior to the UW operation. As discussed in Chapter 2, the turmoil unfolding in the Ukraine capital of Kiev provided Russia with a political opportunity to frame the crisis as requiring Russian action to protect their military personnel and Russian-speaking people in Crimea. Russia had already laid the groundwork for mobilizing structures prior to the UW operation by training and organizing local resistance units and using the Crimean pro-Russian political parties to organize mass protests against the Ukrainian government. Russia masterfully used Internet technologies to push its narrative of events and deceive the world long enough to launch its UW operation. With the UW operation underway, Russia employed a paramilitary force on the ground in Crimea and enhanced their operation by conducting cyberspace operations, annexing Crimea without firing a shot.

The factors that enhanced Russia's social mobilization during the unconventional warfare operation in Crimea that fall within the four selected categories from this case study are highlighted in the analysis framework shown in Figure 6. Although many of these factors are not inherently cyber operations, they all support the Russian's cyber campaign in Crimea.

Figure 6. Crimea Analysis.

D. NON-STATE ACTORS

This case is distinct because it specifically deals with non-state actors' use of cyberspace operations to enhance their recruitment, indoctrination, training and operations in UW-like campaigns that are still ongoing. The other case studies focused on state actors within a specific timeframe where the UW-like campaigns have drawn to a close. This case study will identify how two non-state actors, specifically al-Suri, who was a member of Al-Qaida, and the Al-Qaida offshoot, Islamic State, have and continue to use cyberspace operations in furtherance of their objectives. The case study will start by detailing Al-Suri's life, outlining his jihadi unconventional warfare framework put forth in the *Global Islamic Resistance Call,* and discussing how Al-Suri used cyberspace to enhance the global jihadi movement through collective action. The case will focus on how Islamic State has successfully employed Al-Suri's framework using cyberspace operations with regard to the selected categories of recruitment, indoctrination, training and operations.

On January 9, 2015, Amedy Coulibaly barricaded himself inside a kosher supermarket in Paris, France and executed four Jewish patrons before being killed by Paris police.[186] On May 4, 2015, Elton Simpson and Nadir Soofi opened fire at a cartoon exhibit of the Prophet Muhammad in Garland, Texas, where they were both killed by Texas police.[187] On June 2, 2015, Usaama Rahim was shot and killed near Boston, Massachusetts, when he pulled a military-style knife on a Boston Police officer and Federal Bureau of Investigation (FBI) special agent who had approached him to question him in regard to a plot to behead a police officer.[188] The link between these three events is that the individuals involved were conducting terrorist operations on behalf of Islamic State, even though they had never physically met with it. These individuals' only contact with Islamic State was virtual, through cyberspace.

The events outlined above are the full realization of Al-Suri's *Global Islamic Resistance Call*, which he published online in January 2005. In this work, his *magnum opus*, Al-Suri outlined his blueprint for "a global terrorist campaign against the West that would rely on diffuse, decentralized and non-hierarchical networks."[189] Additionally, he pioneered the term "individual jihad" which "refers to acts of violence carried out by individuals [or small groups] without any organizational adherence."[190] Al-Suri's blueprint is embodied within the three events outlined above and at its core his *Global Islamic Resistance Call* provides a framework for jihadi unconventional warfare that is perfectly tailored for cyberspace and put to full use by the Islamic State.

---

[186] Shiv Malik et al., "Paris Supermarket Attacker Claims Allegiance to Islamic State in Video," *Guardian*, January 11, 2015, http://www.theguardian.com/world/2015/jan/11/paris-supermarket-attacker-islamic-state-video-isis-amedy-coulibaly.

[187] Polly Mosendz, "Report: Shooters at Garland, Texas Muhammad Cartoon Event Linked to ISIS," *Newsweek*, May 4, 2015, http://www.newsweek.com/report-shooters-garland-texas-muhammad-cartoon-event-linked-isis-328267.

[188] Adam Goldman, "Two Men in Boston Charged with Planning to Aid Islamic State," *Washington Post*, June 12, 2015, https://www.washingtonpost.com/world/national-security/two-men-in-boston-charged-with-planning-to-aid-the-islamic-state/2015/06/12/c8cd2c3a-1110-11e5-9726-49d6fa26a8c6_story.html; Evan Allen, Laura Crimaldi, and Lisa Wangsness, "Man Shot, Killed by Law Enforcement in Roslindale Was under 24-Hour Surveillance," *Boston Globe*, June 2, 2015, https://www.bostonglobe.com/metro/2015/06/02/boston-police-officer-shoots-and-wounds-man-roslindale/Akg16CkZJa719BLrBGFOdL/story.html.

[189] Lia, *Architect of Global Jihad*, 6–7.

[190] Ibid., 104.

1. Background

The background for this case study will consist of three sub-sections. The first two will discuss Al-Suri and how his doctrine, *Global Islamic Resistance Call,* can also be seen as an outline for Jihadi unconventional warfare. The third part will outline the Islamic State's use of cyber and unconventional warfare-like activities.

a. Abu Musa'ab Al-Suri the Al-Qaida Strategist

Mustafa bin Abd al-Qadir Sitt Maryam Nasar was born in Aleppo, Syria, in October 1958; he is known to the world by his *nom de guerre* Abu Musa'ab Al-Suri.[191] Al-Suri's life of global jihad began in 1980 when he joined The Combat Vanguard at the age of 21 to fight against the Syrian government.[192] During the 1980s, Al-Suri conducted training in Iraq, Jordan, and Egypt, where he learned military explosive engineering, guerrilla warfare, and special operations.[193] He quickly became an instructor in these subjects and taught in Baghdad, Iraq and Amman, Jordan before seeking exile in Europe, where he published his first work titled *The Islamic Jihad Revolution in Syria,* which was "an analysis of the jihadi movement in Syria."[194]

During the late 1980s, he went to Afghanistan and Pakistan to join the Afghan jihad where he met Osama bin Laden, conducted operations, and was a military instructor at al-Qaida training camps.[195] During the early 1990s, he lived in Spain and London, England where he opened a media center and continued to study and publish works on jihad through print and online media.[196] According to Lia, an expert on Al-Suri, during this time period Al-Suri wanted to improve "the quality and impact of the jihadi groups'

---

[191] Lia, *Architect of Global Jihad*, 30–33; Zackie, "Analysis of Abu Mus'ab Al-Suri's," 1.

[192] Lia, *Architect of Global Jihad*, 37–40.

[193] Ibid., 40–46. Cruickshank and Ali, "Architect of the New Al Qaeda," 1–14.

[194] Lia, *Architect of Global Jihad*, 40–65, 59.

[195] Ibid., 40–88; Cruickshank and Ali, "Architect of the New Al Qaeda."

[196] Lia, *Architect of Global Jihad*, 149–74.

use of the media, which he then considered one of the very greatest gaps in jihadi activity."[197]

During the late 1990s, Al-Suri facilitated media interviews with bin Laden for CNN before leaving London for Afghanistan to work in the service of the Taliban.[198] Starting in 1999 and over the course of the following year, Al-Suri established a media and research center and the al-Ghuraba training camp with the permission of the Taliban near Kabul, Afghanistan.[199] At these two locations, Al-Suri began to deliver lectures about his ideas of "autonomous cells de-linked from any identifiable organizational structure, and whose main method of operation should be individual terrorism," thus propagating his framework for jihadi unconventional warfare, which would be published in its entirety several years later in the *Global Islamic Resistance Call*.[200] Sometime after the 9/11 attacks, Al-Suri fled to Pakistan where he isolated himself and devoted his time to reflection and finalizing the *Global Islamic Resistance Call,* which he completed in late 2004.[201] In November 2005, Pakistani police arrested Al-Suri who had a $5 million USD bounty on his head from the U.S. Department of State.[202]

b. Global Islamic Resistance Call – Framework for Jihadi Unconventional Warfare

Al-Suri's publication of the *Global Islamic Resistance Call* is grounded in his two-and-a- half decades of jihadi experience ranging from student, trainer, operator, and military strategist. This seminal jihadi unconventional warfare framework has earned Al-Suri titles and nicknames such as "al-Qaida's leading theoretician and strategic thinker," "architect of global jihad," "the world's foremost jihadi theoretician," "the pen jihadist"

---

[197] Lia, *Architect of Global Jihad*, 151.

[198] Ibid., 165–70, 229–78.

[199] Ibid., 246.

[200] Ibid., 256–57.

[201] Ibid., 317–24.

[202] Cruickshank and Ali, "Architect of the New Al Qaeda;" U.S. Department of State, Bureau of International Information Programs, "U.S. Offers $5 Million Reward for Information about Terrorist," *GlobalSecurity.org*, November 18, 2004, http://www.globalsecurity.org/security/library/news/2004/11/sec-041118-usia01.htm.

and "Castro."[203] Al-Suri saw "himself as a jihadi strategist, theoretician, and thinker, rather than an ideologue and a cleric" and grounded his work in the guerrilla strategies of Mao Tse-tung, Fidel Castro and Che Guevara.[204]

In an article titled "An Analysis of Abu Mus'ab al-Suri's *Call to Global Islamic Resistance*," Zackie discusses Al-Suri's 1,600-page, two-part book. He summarizes the first part, *Roots, History and Experiences,* as dealing with Muslim history, the struggle with the West, and recent jihadi struggles all rooted within a political, social, and legal context.[205] Zackie concluded that the first part provides what Al-Suri hopes is a narrative to compel popular embrace of his call for global Islamic resistance, leading the reader to the second part, *Call, Methodology, Way*. He says that this second part, which "details the theoretical frameworks that…essentially [is] a plan of action that addresses the work to be done on the political, educational, military, financial, and media fronts," is in essence Al-Suri's jihadi unconventional warfare framework.[206]

Within this jihadi unconventional warfare framework, Al-Suri advocates two main concepts to accommodate the United States' superior technological military advantages in a post 9/11 world: "individual jihad and small cell terrorism" and "a system, not a secret organization."[207] Al-Suri describes individual jihad and small cell terrorism as "…single operations…carried out by individuals or small groups" that are decentralized and do not adhere to hierarchical organizational structures.[208] Al-Suri's second main concept, usually referred to as "a system, not a secret organization" may be translated literally from Arabic as "system of action, not a centralized, secret organization

---

[203] Zackie, "Analysis of Abu Mus'ab Al-Suri's," 1; Lia, *Architect of Global Jihad*; Jarret M. Brachman and William F. McCants, "Stealing Al Qaeda's Playbook," *Studies in Conflict & Terrorism* 29, no. 4 (July 2006): 314, doi: 10.1080/10576100600634605.

[204] Lia, *Architect of Global Jihad*; Sarah E. Zabel, "The Military Strategy of Global Jihad," Strategic Studies Institute, October 2007, 9, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB809.pdf.

[205] Zackie, "Analysis of Abu Mus'ab Al-Suri's."

[206] Ibid.

[207] As translated by Lia, Abu Mus'ab al-Suri, Global Islamic Resistance Call published online in Arabic, January 2005, p. 1355-1413, as cited in Lia, *Architect of Global Jihad*, 347–440.

[208] Ibid., 351.

for action."[209] Al-Suri states, "[t]he idea is based on the concept that the bonds between the entire spectrum of Resistance fighters – individuals, cells, units and small groups – are limited to…[a]…program of beliefs, a system of action, a common name, and a common goal" and further elaborates there should not be any connections between "Resistance Fighters."[210]

In summary, Al-Suri's *Global Islamic Resistance Call,* "…invites its readers to self-recruit and become independent terrorists…" which, individuals can now do through cyberspace and from the comfort of their own home without ever physically meeting one another. This modern technological enhancement to UW has been lethally demonstrated in the events outlined in the beginning of this chapter by the Islamic State.[211] In addition to creating a jihadi unconventional warfare framework, Al-Suri called for and used technology, specifically cyberspace, to reach the masses and enhance the jihadi resistance movement, which al-Suri promoted in the areas of recruitment, indoctrination, training and operations.

c. The Islamic State

The Islamic State, as it is now known, is a terrorist organization that morphed from an Al-Qaeda offshoot to its current form, controlling large areas of territory in Syria and Iraq and administering a de-facto state-like enterprise with a borderline standing army.[212] The analysis of the Islamic State within this chapter is limited in scope to its use of cyberspace operations for the purposes of recruitment, indoctrination, training and operations. The Islamic State has successfully implemented Al-Suri's jihadi unconventional warfare framework by having individuals self-recruit, self-indoctrinate, and self-train, all via cyberspace, and then conduct "individual jihad" (known in the U.S. as "lone wolf attacks").[213]

---

[209] Lia, *Architect of Global Jihad*, 421.

[210] Ibid., 421–22.

[211] Zackie, "Analysis of Abu Mus'ab Al-Suri's."

[212] Jessica Stern and J.M. Berger, *ISIS: The State of Terror* (New York: HarperCollins, 2015).

[213] Ibid.

2. Operations

This section is broken into two parts. The first will describe the Al-Suri model for exploitation of cyberspace for the purposes of global Jihad. The second part will describe how the Islamic State uses cyberspace to enhance their operations.

a. Al-Suri's Use of Cyberspace

Al-Suri is credited with being "the chief architect of al-Qaeda's contemporary Internet movement" because he advocated using cyberspace to provide the means for individuals to self-recruit, self-indoctrinate, and self-train.[214] With these cyber-enabled capabilities any jihadi can than conduct an operation, if they so choose.

Al-Suri used his own website, *The Library of Shaykh Umar Abd al-Hakim-Abu Mus'ab al-Suri: Your Guide to the Way of Jihad,* and other online jihadi forums to publish written works, lectures via video, and audio files with the intent to recruit and indoctrinate individuals.[215] Additionally, Al-Suri used cyberspace to train individuals by publishing jihadi military doctrine and "how to" videos and lectures on guerrilla warfare.[216]

Early in the 1990s, Al-Suri recognized the power of cyberspace and the benefits it could provide to those who harnessed it. Although he does not use the term "Collective Action,"[217] his numerous online works culminating with his *Global Islamic Resistance Call,* provide the ideological foundation to overcome the "start-up problem" - when people look past their individual motivations and participate in a larger group behavior - "individual jihad" combined with "a system."[218] More than a decade has passed since Al-Suri's *magnum opus* was published, and no other non-state actor has been more

---

[214] Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *Fletcher Forum of World Affairs* 30, no. 2 (summer 2006): 159.

[215] Lia, *Architect of Global Jihad*, 29, 259–74.

[216] Ibid., 259–274.

[217] Centola, "Homophily, Networks, and Critical Mass," 3–40; Olson, *Logic of Collective Action*; Ostrom, "Behavioral Approach;" Ostrom, "Analyzing Collective Action," 155–66; Ostrom, "Collective Action and the Evolution," 235–52.

[218] Ibid.

successful in using cyberspace to recruit, indoctrinate, train, and operationalize "individual jihad" than the Al-Qaeda offshoot, the Islamic State.[219]

b. The Islamic State's Use of Cyberspace

The Islamic State uses social media as the cornerstone of its cyberspace operations and "its innovative and aggressive approach has afforded it an unprecedented level of success."[220] The Islamic State appears to have cracked the code on the conditions required for social mobilization via the Internet in regards to recruiting, indoctrinating, and training, leading directly to operations. During testimony at *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment* on May 7, 2015 before the U.S. Senate Committee on Homeland Security and Government Affairs, Berger highlighted how, "since the beginning of 2015, at least 30 Americans in 13 States have been subject to law enforcement action for attempting to join ISIS or carry out violence inspired by ISIS. In every case, a significant social media component was found in the radicalization [indoctrination] or recruitment process."[221]

Another cyberspace operation employed by the Islamic State is the production and distribution of its own slick and flashy magazine called *Dabiq*. This magazine is available in several languages including English and published on the Internet mainly to recruit and indoctrinate individuals.[222]

The Islamic State is also a prolific user of Facebook, YouTube, and Twitter, which are designed to connect individuals and deliver content via the Internet, to recruit, indoctrinate and train individuals.[223] Cinema-quality propaganda videos are produced

---

[219] Christoph Reuter, "The Terror Strategist: Secret Files Reveal the Structure of Islamic State," *Spiegel Online International*, April 18, 2015, http://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html; Stern and Berger, *ISIS: State of Terror*, 1–385.

[220] J.M. Berger, "Social Media: An Evolving Front in Radicalization," U.S. Senate Committee on Homeland Security & Governmental Affairs, May 7, 2015, http://www.hsgac.senate.gov/hearings/jihad-20-social-media-in-the-next-evolution-of-terrorist-recruitment.

[221] Ibid.

[222] "The Islamic State's (ISIS, ISIL) Magazine," Clarion Project, September 2014, http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq.

[223] Berger, "Social Media;" Stern and Berger, *ISIS: State of Terror*, 147–76.

and posted to these social media sites allowing for individuals to self-recruit, self-indoctrinate, and self-train. Additionally, the Islamic State uses private social media platforms, such as Kik and WhatsApp, and private Facebook messages, to conduct more sensitive conversations and perhaps recruiting and planning operations abroad.[224] The Islamic State has become so successful at recruiting individuals through social media from a continent or two away, that the U.S. National Counterterrorism Center's Zafar coined the term "peer-to-peer recruiting" to call attention to the phenomenon.[225]

The Islamic State even created its own app in April 2014, titled "Dawn of Glad Tidings," which provided users with exclusive Islamic State content and allowed users to post the content to their Twitter account.[226] Behind the scenes and unknown to the users, the Islamic State app collected users' personal data as well as revenues through advertising.[227] Additionally, when used with a Twitter app, the Islamic State app could be automatically set up by users to re-tweet content and also contained "…computer code that could take control of a consenting user's account to automatically send out tweets."[228] By December 2014, the Islamic State had created thousands of computer "bots," most of which were used to automatically tweet links and videos of sensational propaganda, such as beheadings, in order to recruit and indoctrinate individuals to their cause.[229]

3. Summary

Cyberspace provides the Islamic State with an infinite number of potential recruits with the only limiting factor being an Internet connection. Al-Suri and the Islamic State have provided the means for individuals with an Internet connection to self-

---

[224] Berger, "Social Media."

[225] Stern and Berger, *ISIS: State of Terror*, 159; Shaarik H. Zafar, "Western Foreign Fighters in Syria: Implications for U.S. CVE Efforts," *Washington Institute for Near East Policy*, March 14, 2014, http://www.washingtoninstitute.org/policy-analysis/view/western-foreign-fighters-in-syria-implications-for-u.s.-cve-efforts.

[226] Stern and Berger, *ISIS: State of Terror*, 147–51.

[227] Ibid., 159.

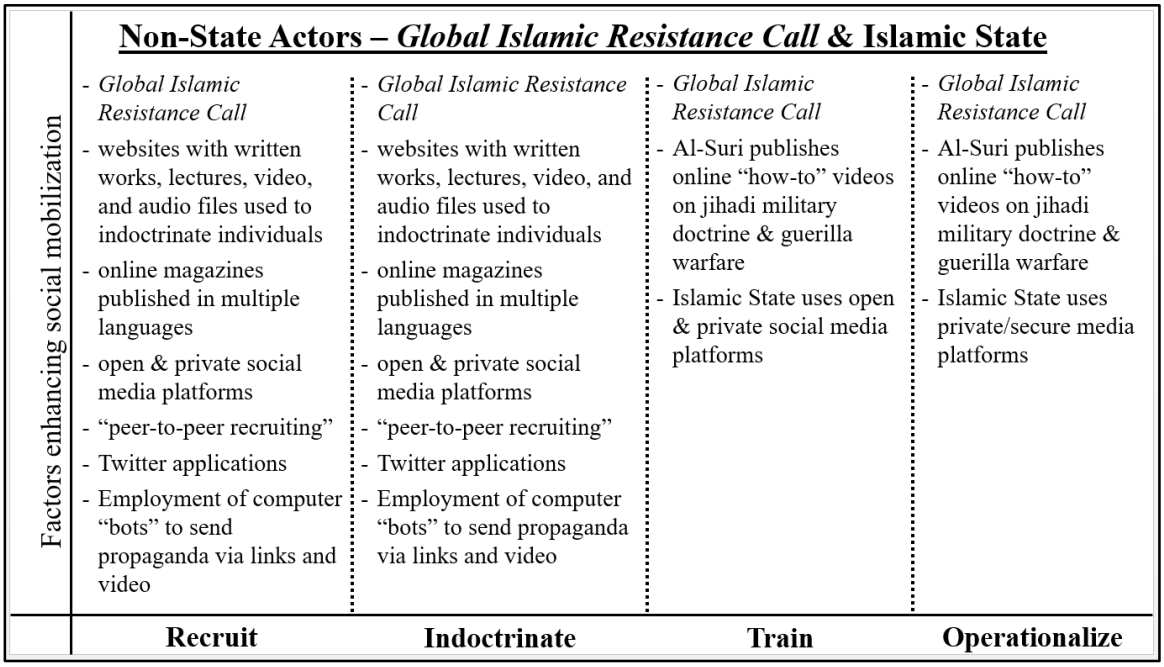
[228] Ibid., 149.

[229] Ibid., 150–51.

recruit, self-indoctrinate, and self-train through platforms such as online publications, Facebook, YouTube, Twitter, and WhatsApp. The Islamic State has proven through events in Paris, Garland, and Boston, that individuals do not have to physically travel to Iraq and Syria to fight on behalf of the Islamic State but can conduct "individual jihad" through means available in cyberspace, in the cities and countries from which they connect to the Internet.

Al-Suri's and the Islamic State's use of cyberspace operations to conduct unconventional warfare-like operations in the four selected activities from this case study are highlighted in the analysis framework shown in Figure 7.

Figure 7. Non-state Actor Analysis.



IV. ANALYSIS

The previous chapters of this thesis show that social mobilization is critical to understanding the theoretical underpinnings for why individuals would accept the severe risks of joining an insurgent organization for the purpose of conducting UW. Through a comprehensive literature review, four areas of activity were examined to determine what conditions, present in the cyberspace environment, could enhance the conduct of UW. By conducting an examination across the four distinct cases, through the lens of the four activities, we were able to find evidence to support our two claims and identified five additional conditions that existed for cyber-enabled UW.

The first section of this chapter examines the two claims and identifies the evidence supporting them. The second section describes five similar conditions that were present across the cases and enhanced the conduct of cyber-enabled UW. The third section describes how Social Network Analysis has the potential to enhance a cyber-enabled UW organization across the four activities analyzed. The fourth section of this chapter recommends the organization, structure, training, and equipment of a hypothetical cyber-enabled UW team. The final section examines the barrier between the cyber and physical domains and how they can be influenced by cyber-enabled UW operations.

A. CLAIMS

1. Virtual Environment and Social Mobilization

Our first claim, that a low cost of entry, sparse regulations, and anonymity of users in the virtual environment facilitates social mobilization and recruiting of proxy forces during cyber-enabled UW operations, was supported by evidence contained in the two Russian case studies and the case study involving non-state actors. Russia exploited the cyber domain in both Georgia and Ukraine, using a combination of proxy cyber forces to mobilize populations both in the cyber and physical domains. In the case involving non-state actors, both Al Suri and the Islamic State used cyberspace to mobilize populations through websites, chat rooms, and online publications. Individuals that were

mobilized, whether as part of "troll armies" or "peer-to-peer" recruiting, incurred a minimal cost to participate. All that was required was an Internet capable device and an Internet connection, limited regulation, and massive anonymity when using private and secure media platforms and software. Cyberspace enhanced the social mobilization factors within each case study and demonstrated the effectiveness of recruiting proxy forces, specifically during cyber-enabled UW operations.

2. Cyberspace as a Platform for Unconventional Warfare

Claim two, which asserts that the speed of information and the vast amount of multi-media content makes cyberspace an excellent platform for UW resistance groups to organize, train, and conduct operations, is supported by evidence from the three case studies that employed cyber-enabled UW-like operations. The case studies demonstrate that numerous cyberspace platforms were used, including online "how to" videos, social media platforms, and specially designed "apps" (both by the Russians and non-state actors) to organize, train, and conduct operations. The Islamic State appears to have mastered this skillset and is able to fully recruit, train, and operationalize individuals via cyberspace to carry out operations on the other side of the globe without ever physically meeting those conducting the operation. UW organizations only need to have the ability to put content out into cyberspace, which if done correctly, can almost instantaneously reach any user in the world with an Internet connection. The case studies firmly demonstrate that numerous platforms available in cyberspace, if harnessed correctly, can be used for UW resistance groups to organize, train, and conduct operations.

B. CYBER-ENABLED UW CONDITIONS PRESENT IN THE CASES

Unconventional Warfare is not new. What is new is the advent of cyberspace and the ability for like-minded people or organizations to connect with one another and to reach a mass audience like never before. Cyberspace has enhanced the ability of people to mobilize from anywhere in the world, and all that is required is a cheap smart phone and a free WiFi connection. The case studies demonstrate that five similar conditions are present across the activities analyzed, (recruitment, indoctrination, training, and

operationalizing), which support successful cyber-enabled UW-like operations, in addition to the two claims above.

A common condition that was present across all four case studies and the UW activities analyzed was that an ethnic, cultural, or ideological similarity existed between the individuals that partook in the social mobilization and the UW-type organization that led the operation. Prior to the advent of cyberspace, as demonstrated in the Detachment 101 case, the conductors of UW would have to meet in-person to build upon the social mobilization that occurred in order to recruit, indoctrinate, train, and conduct operations. Cyberspace provides the capability for individuals of an ethnic, cultural, or ideological similarity to meet virtually, from halfway around the world through numerous social media sites, with the click of a few buttons.,

The second condition present across the four cases was that the actors conducting the UW-like operation felt that it was a legitimate action and the cause was just. Legitimacy is extremely important for any UW operation and manifested itself in similar ways across the cases. Legitimacy was reinforced in the Russian case studies by drawing on ethnic and cultural components and in the non-state actor case study through ideology, specifically Al-Suri's *Global Islamic Resistance Call*. Cyber-enabled UW allows individuals of a similar ethnic, cultural, or ideological identity to participate in a perceived to be legitimate UW-like operation without actually physically showing-up on the battlefield, if they so choose.

The third condition was the exploitation of existing groups, organizations, or networks to assist in conducting UW-like operations, with cyberspace providing numerous opportunities that otherwise would not have existed. In the South Ossetia case, Russia used proxies to facilitate operations on the cyber battlefield and the RBN advanced software and hacking techniques against Georgia. In Crimea, Russia used "troll armies" to spread the Russian narrative of events through numerous social media platforms. The non-state actor case showed that Al-Suri published his *Global Islamic Resistance Call* and jihad and guerrilla warfare "how to" videos on the Internet, instantly available to anyone with an Internet connection. The Islamic State successfully employed computer "bots" to send propaganda via web-links and video. Cyber-enabled UW allows

an actor to leverage cyberspace capabilities that are not otherwise available to them and reach a mass audience with ease.

A fourth condition observed in the three most recent case studies was the existence of a susceptible population that was connected to the Internet. Cyberspace reduced barriers to, and increased the reach of, the UW organizations to engage susceptible populations within the activities of recruitment, indoctrination, training, and conducting UW-like operations. The Islamic State appears to be the most successful in cyber-enabled UW-like operations and exploiting this condition. This pseudo-state creates and publishes Dabiq, their online magazine in multiple languages to indoctrinate individuals. They use "peer-to-peer" recruiting as well as open and private social media platforms to recruit and train individuals. These individuals then conduct UW-like operations on behalf of the Islamic State without ever physically meeting an Islamic State trainer or recruiter, as showcased in Garland, Texas. Cyber-enabled UW reduces the barrier to any participant and increases their potential reach to susceptible populations as long as both parties have some sort of Internet connection and a basic web-surfing device.

The fifth and final condition that presented itself was that the nature of the conflict itself had to be such that Unconventional Warfare was an appropriate strategy to achieve the desired outcomes. The timeframe of the conflict must be expansive enough to allow for UW-like operations, although this timeframe has the potential to be compressed for cyber-enabled UW. The social environment must be conducive and complex enough to allow a UW-type organization to exploit the sympathetic social fragmentations in favor of the UW organization. A cyber-enabled UW approach will allow for a more expansive and flexible exploitation of sympathetic groups than has previously been possible.

With these seven conditions present, cyber-enabled UW may reduce the risk and the cost of conducting UW-like operations. Within both Russian case studies, Putin's proxies conducted successful cyber-attacks against both Georgia and the Ukraine command and control and critical infrastructures, rendering them useless during the UW operations. Prior to the advent of cyberspace, Russia would have had to risk men and military hardware to achieve the same results. Now all that is needed is a trained cyber-

operator, a laptop, and an Internet connection. The Islamic State also demonstrated the reduced risk and cost of conducting cyber-enabled UW-like operations. The Islamic State's creation and employment of the Twitter app, Dawn of Glad Tidings, demonstrated that for a very low cost to the organization, they could potentially reach anyone on Twitter. Cyber-enabled UW reduces the risk and cost of conducting operations through cyberspace to the UW organization both in terms of potential lives on the line and resources required to accomplish stated objectives.

Cyber-enabled UW has implications for providing delayed attribution and enabling anonymous action. This allows for control over the conflict narrative. If the conflict narrative is controlled the UW organization can share, obscure, or manipulate information with certain parties at a time of their choosing. This can enhance a UW organization's flexibility within the political and diplomatic arenas. Russia's use of cyber-enabled UW to annex Crimea showcases the ways in which attribution can be controlled and the narrative shaped to further a political agenda.

C. THE POTENTIAL OF SOCIAL NETWORK ANALYSIS

Although the case studies do not specifically identify any cyber-enabled UW team employing SNA as described in Chapter II, one could only imagine the power this technique could unleash for a UW organization. SNA techniques and software have the potential to enhance a cyber-enabled UW team's capabilities to identify evaluate, indoctrinate, and recruit proxy forces. Even though none of the case studies uncovered the use of SNA, evidence was provided showing numerous social media platforms and specially designed software were used during the three cases that employed cyber-enabled UW-like operations. These platforms and special software were directed towards an intended target audience in order to recruit, indoctrinate, train, and eventually operationalize proxy forces. Given the success of the cyber-enabled UW-like operations identified in the case studies, even though they did not employ SNA, using these techniques could have potentially enhanced their efforts.

Using commercial of the shelf SNA software, a cyber-enabled UW team could target and scrape data from publically available social media sites, information from

websites, and identify networks that already exist which could be used as potential proxy forces. This targeted approach using SNA techniques and software would increase the cyber-enabled UW team's ability to quickly and more accurately identify, evaluate, indoctrinate, and recruit proxy forces when compared to the techniques effectively demonstrated in the case studies.

D. A CYBER-ENABLED UW TEAM

The previous section of this chapter describes the base conditions that are necessary to exploit the cyber environment to enhance the execution of UW. Understanding these conditions is the key to operationalizing a force to exploit concepts uncovered in previous chapters. In addition, it is necessary to determine the organization, training, and equipment needed to conduct cyber-enabled UW.

To develop a preliminary concept for what a cyber-enabled UW team should consist of, two commands of the U.S. military need to be examined. The first of these commands is the United States Cyber Command (USCYBERCOM). The second is the United States Special Operations Command (USSOCOM) and its subordinate the United States Army Special Operations Command (USASOC). The following two sections will look at each of these commands to determine if the requisite capabilities necessary for cyber-enabled UW are present in existing organizations. A third section will recommend the ideal structure, training, and equipment for a cyber-enabled UW team.

1. USCYBERCOM

USCYBERCOM is the U.S. military's proponent organization for all offensive and defensive operations conducted in cyberspace. In addition, it is also responsible for all Department of Defense Information Networks (DODIN).[230] This command's responsibilities and authorities overlap with organizations that conduct Electronic Warfare (EW) and Information Operations (IO). Although significant overlap exists, USCYBERCOM doctrine does not specifically reference Special Operations except as a

[230] Joint Chiefs of Staff, *Cyberspace Operations* [JP 3-12 (R)].

force and equipment provider.[231] According to their mission statement, USCYBERCOM first and foremost is concerned with enabling and protecting DODIN. In addition, they will protect U.S. military maneuvers in cyberspace and deny the same to our enemies.[232]

Cyber doctrine does not address UW operations supported through cyberspace, nor does it allocate forces for such a purpose.[233] Forces associated with cyber organizations in the U.S. military continue to grow exponentially, but USCYBERCOM does not have an organization, currently in its ranks, that is prepared for, or that could be tailored for the purpose of supporting cyber-enabled UW.[234]

This being said, USCYBERCOM is a critical organization that needs to be leveraged for the training and equipping of a cyber-enabled UW team. USCYBERCOM's focus on advanced techniques and technologies necessary to operate in the complex cyber domain will act as a critical enabler to cyber focused UW forces. One of the first, and enduring, tasks of a proposed cyber-enabled UW team will be to establish and maintain a positive relationship with USCYBERCOM and its subordinate service elements (particularly Army Cyber Command). This relationship will enable a UW focused team to have the latest intelligence, technologies, and techniques to identify and exploit conditions present in the cyber environment for the purposes of recruiting, indoctrinating, training, and operationalizing proxy forces prior to physical infiltration of U.S. troops.

2. USSOCOM and USASOC

USSOCOM is responsible for the conduct of operations to enable resistance and insurgent organization for a variety of purposes described in detail in previous chapters of this thesis. Tasks conducted within these operations are broadly referred to as UW. USSOCOM has tasked USASOC as the proponent command for the conduct of UW per

---

[231] Ibid.

[232] "USCYBERCOM," U.S. Army Cyber Command, accessed October 25, 2015, http://www.arcyber.army.mil/org-uscc.html.

[233] Joint Chiefs of Staff, *Cyberspace Operations* [JP 3-12 (R)].

[234] Cheryl Pellerin, "Cybercom Chief: Cyber Threats Blur Roles, Relationships," *Department of Defense News*, March 6, 2015, http://www.defense.gov/News-Article-View/Article/604225; Joint Chiefs of Staff, *Cyberspace Operations* [JP 3-12 (R)].

the command's directive 10–1.[235] Additionally, joint special operations doctrine assigns U.S. Army Special Forces additional importance in conducting UW.[236]

The base unit of action for a Special Operations Group (under USASOC) is a Special Forces Operational Detachment Alpha (SFODA). This small unit is uniquely organized, trained, and equipped to achieve strategic effects through operations conducted at the tactical and operational levels. An SFODA consists of twelve individuals that receive extensive training in tactics and weapons, intelligence, engineering, demolition, communication, and medical operations.[237] Although UW is a prominent feature in both joint and army special operations doctrine, integration of cyber capabilities, or the conduct of UW in the cyber domain, is not included in current manuals.[238] Given the current lack of skills necessary for the conduct of UW operations in the cyber domain, an SFODA would need a substantial amount of advanced training and equipment to achieve proficiency in this very different domain of warfare. Special Forces (SF) operators are specifically selected and trained for flexibility in complex environments, but adding additional (primarily technical) capabilities would change the nature of the unit. This suggests that a new organization should be considered to enhance and contribute to an SFODA's ability to conduct UW operations in the cyber domain.

3. A New Unit

The previous two sections reveal that an organization specifically tailored to exploiting the cyber environment to enhance UW goals currently does not exist. To better exploit the conditions identified in previous chapters, a new organization should be

---

[235] United States Special Operations Command, *Organization and Functions: Terms of Reference--Roles, Missions, and Functions of Component Commands*, USSOCOM Directive 10-1 (MacDill Air Force Base, FL: United States Special Operations Command, 2009), https://jsou.blackboard.com/bbcswebdav/library/Library%20Content/JSOU%20References/JSOU-ISOF/ISOF%20References/USSOCOM%20Directive%2010-1%2015%20Dec%2009.pdf.

[236] Joint Chiefs of Staff, *Special Operations* (JP 3-05), GL-10.

[237] Department of the Army, *Army Special Operations Forces* [FM 3-05 (FM100-25)].

[238] Department of the Army, *Army Special Operations Forces* [FM 3-05 (FM100-25)]; Department of the Army, *Army Special Operations Forces Unconventional Warfare* (FM 3-05.130); Department of the Army, *Special Forces: Unconventional Warfare* (TC 18-01); Joint Chiefs of Staff, *Special Operations* (JP 3-05).

considered for this purpose. This new element would be built to support an SFODA, which receives extensive training on UW theory and practice. Although the SFODA would be heavily involved in recruiting, indoctrinating, training, and ultimately operationalizing digital networks, the unit's main purpose is continuing these functions in the physical world (if and when a UW operation crosses the cyber to physical boundary). Additionally, an extensive network of personnel involved in both cyber operations (at USCYBERCOM), UW experts (at USSOCOM and USASOC), and interagency partners should be formed. This network will support and facilitate all cyber-enabled UW operations and considerably reduce any operational overlap between the commands and other interagency organizations.

Duggan suggests that the core element for a cyber UW team should be built around the currently existing army SF team. In this concept, a "cyber-pilot team" would prepare the environment in a host country through cyberspace, drastically reducing the risks that physical infiltration into enemy territory would otherwise entail. In his model, the same team that conducted these initial tasks would also physically deploy forward once the environment and insurgent organizations were sufficiently prepared.239 Depending on the size and dispersion of forces, one or more SFODAs could be required to infiltrate into the UW operational area.

In order to not lose continuity in the digital world, once a physical deployment is deemed necessary, it would be unwise to use an SFODA, which is uniquely trained and equipped to execute UW in the physical world. In order to mitigate this, a new cyber-enabled UW team needs to be established. This team needs to reside within USASOC and directly support a Special Forces Group's UW activities. Potentially, the cyber-enabled UW team could fall under a Special Forces Group's Support Battalion or a Psychological Operations Battalion.

This purely cyber-focused team would be primarily staffed with regionally focused Special Operations Forces personnel. Additionally, a host of military and interagency enablers would be necessary to advise and support the team. SMT, SNA, and

239 Patrick Michael Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly*, no. 79 (2015): 46–53.

online social media experts from the military, interagency community, and academia would help the team exploit factors that lead to social mobilization. Linguists and cultural experts are critical to creating believable content that aids in cyber-enabled UW tasks. Additionally, Geospatial intelligence experts could assist in mapping the complex human and physical infrastructure discovered through cyberspace. Military or interagency personnel capable of conducting cyber and real world human intelligence support operations are also critical enablers. Offensive and defensive cyber capabilities, resourced through USCYBERCOM and the National Security Agency, will be critical in enhancing the legitimacy of an insurgent organization as well as diminishing the legitimacy of the incumbent government.

The enablers described in the previous paragraph are by no means a complete list. Based on the nature and scope of the UW operation, additional capabilities may be necessary. A credible unit for conducting cyber-enabled UW operations does not currently exist, and therefore needs to be formed and tested to better understand the exact organization, training, and equipment required to support UW operations.

E. CROSSING THE THRESHOLD

Cyber-enabled UW teams can utilize the conducive environment provided by the Internet to produce content that will draw members of potential or existing resistance organizations together. These teams can additionally identify intelligence, operational information, and psychological factors that are present in the UW environment. Then teams can passively select potential members that are drawn to this content. After prospective recruits, groups, or networks are selected, indoctrination can begin.

Next, virtual training of recruited individuals and groups commences. This training includes the distribution of materials that will enhance the resistance posture of these groups in both kinetic and non-kinetic techniques, to include (but not limited to) sabotage, subversion, and non-violent resistance techniques. Additional organization of revolutionary groups is also possible utilizing online techniques, but may require a physical presence if complete control of the organization is desired. Building the network

of an UW group is possible using only cyber means, but the larger the network becomes the more difficult it is to maintain control.

Finally, a call to action is a key step when operationalizing UW groups. This key step, while possible through the virtual world, is not likely to occur without the introduction of personnel to facilitate additional coordination with groups in the physical world. This is the point where an SFODA would need to deploy, if one has not already infiltrated into the area of operations, to continue the UW operation. However, even when this digital to physical boundary is crossed, the work of the digital team must continue. Maintaining an online UW presence will not only inform the physical team in theater, it will also continue to build, maintain, and organize resistance groups and activities that fall outside of the spectrum of control of the UW focused SFODA in the host country.

At some point, in the course of a cyber-enabled UW campaign, planners have to assess the risk of not having operators physically on the ground, necessary to increase control over proxy forces conducting UW activities. The exact nature of the digital to physical boundary will differ depending on a multitude of factors in the operating environment. Although an operation where UW tasks can be executed completely in the cyber domain is entirely possible, the vast majority of operations will most likely require the physical deployment of U.S. forces. Despite this fact, conducting cyber-enabled UW operations will enable U.S. UW professionals to impact a mature theater when physical infiltration is not a viable option. When an SFODA is deployed in support of a UW operation, the relationship with cyber-enabled UW team must be built and maintained. This mutually supporting relationship will facilitate the coordination between the digital and physical UW efforts. Constant communication between these two teams will help to eliminate mission overlap and ensure continuity of efforts. This, in turn, will reduce the physical risk to soldiers on the ground and the political risk to policymakers.

Since no organization with the requisite capabilities to exploit conditions in the cyber domain to enhance UW currently exists, one should be created. This team will require specialized education in social mobilization theory, training in advanced cyber and UW techniques, specialized equipment, and legal authorities. The core of this team should come from the Army SOF community since they are the military UW proponent

organization. Additional enablers will need to come from the military cyber force, academia, and the broader interagency community. To be successful, this organization will need to be comprised of a wide range of both military and civilian professionals with a diverse range of skillsets.

The mission that would be conducted by a cyber-enabled UW team could potentially overlap with missions of other organizations in USCYBERCOM, USSOCOM, and other interagency organizations. To avoid duplication of effort between organizations, a requirement for cyber capabilities, in support of UW operations, should be created by USSOCOM. A cyber-enabled UW team can then be staffed by the best qualified military, interagency, and civilian organization. Once created, the team should be permanently tasked to support USASOC and their organic UW focused SFODAs. This will streamline authorities and negate any potential organizational infighting. Creating, staffing, training, and equipping a cyber-enabled UW team will not be an easy task. It will require an immense amount of networking and coordination between multiple high-level military commands, interagency organizations, and potentially require input from national level policymakers. Training and equipping the group will also be an arduous, and perhaps, cumbersome process. Despite these obstacles, cyber-enabled UW will provide U.S. leadership with additional options to achieve its foreign policy goals.

V. CONCLUSION

The first section of this chapter will summarize the seven conditions identified through the evidence provided in the cases that can enhance unconventional warfare through cyberspace operations - cyber-enabled UW. The second section recommends the creation of a cyber-enabled UW team and the final section will propose possible avenues of further research.

A. CONDITIONS FOR CYBER-ENABLED UW

This research indicates, through the four cases analyzed, that seven conditions exist in the cyberspace environment that can enhance the conduct of UW. The first condition present was that a low cost of entry, sparse regulations, and anonymity of users in the virtual environment facilitates social mobilization and recruiting of proxy forces during cyber-enabled UW operations. The second condition that presented itself was that the speed of information and the vast amount of multi-media content makes cyberspace an excellent platform for UW resistance groups to organize, train, and conduct operations. A third condition identified that an ethnic, cultural, or ideological similarity existed between the individuals that partook in the social mobilization and the UW-type organization that led the operation. The fourth condition evident was the importance of legitimacy, specifically that actors conducting the UW-like operation felt that it was a legitimate action and the cause was just. The fifth condition was the exploitation of existing groups, organizations, or networks to assist in conducting UW-like operations, with cyberspace providing numerous opportunities that otherwise would not have existed. The sixth condition present in the three most recent case studies was the existence of a susceptible population connected to the Internet. A final and important condition that manifested itself was that the nature of the conflict itself had to be such that UW was an appropriate strategy to achieve the desired outcomes.

These seven conditions should be exploited by UW practitioners to identify counter-state organizations that support the goals of U.S. military and policy makers. By conducting many of the preliminary tasks of UW in the cyber domain, the timeframe for

physically deploying troops to enemy held territory could be pushed significantly into the latter phases of an operation or campaign. Additionally, even when it becomes necessary to deploy soldiers into an UW theater, deployed teams will benefit from a more developed and mature operating environment.

B. CYBER-ENABLED UNCONVENTIONAL WARFARE TEAM

No cyber-enabled UW team currently exists. An organization with the requisite capabilities to exploit the conditions previously identified in the cyber domain should be created. This team will require specialized education in social mobilization theory, training in advanced cyber and UW techniques, specialized equipment, and legal authorities. The core of this team should come from the Army SOF community since they are the military UW proponent organization. Additional enablers will need to come from the military cyber force, academia, and the broader interagency community. To be successful this organization will need to be comprised of a wide range of both military and civilian professionals with a diverse range of skillsets.

The mission of this proposed cyber-enabled UW team could potentially overlap with missions of USCYBERCOM, USSOCOM, and other interagency organizations. To avoid duplication of effort between organizations, a requirement for cyber capabilities, in support of UW operations, should be created by USSOCOM. A cyber-enabled UW team can then be staffed by the best qualified personnel from the military, interagency, and other civilian organization. Once created, the team should be permanently tasked to support USASOC and their organic UW focused SFODAs. This will streamline authorities and negate any potential organizational infighting. The creation of a cyber-enabled UW team will require an immense amount of coordination between multiple high-level military commands, interagency organizations, and potentially require input from national level policymakers. Training and equipping the group will also not be easy. Despite these obstacles, cyber-enabled UW will provide U.S. leadership with additional options to achieve its foreign policy goals.

C. FURTHER RESEARCH

The scope of this research did not fully address all aspects pertinent to the creation and sustainment of a cyber-enabled UW capability. Additional research should first, and foremost, focus on validating the conditions and evidence examined in this research. Further research should analyze the authorities necessary to conduct covert and clandestine operations on foreign soil and in cyberspace. The topics of plausible deniability, low visibility operations, and commercial cover operations should be considered when conducting a review of requisite authorities. This thesis also did not adequately address the full range of organizations that conduct operations in the cyber domain. In order to fully train, equip, and staff a cyber-enabled UW organization, it would first be necessary to understand the current range of capabilities being employed by U.S. cyber professionals. Finally, a review of ethical and legal cyber activities and what would not be ethical and legal requires further understanding for cyber-enabled UW.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Evan, Laura Crimaldi, and Lisa Wangsness. "Man Shot, Killed by Law Enforcement in Roslindale Was under 24-Hour Surveillance." *Boston Globe*, June 2, 2015. https://www.bostonglobe.com/metro/2015/06/02/boston-police-officer-shoots-and-wounds-man-roslindale/Akg16CkZJa719BLrBGFOdL/story.html.

Allison, Roy. "Russian 'Deniable' Intervention in Ukraine: How and Why Russia Broke the Rules." *International Affairs* 90, no. 6 (November 2014): 1255–97. doi: 10.1111/1468-2346.12170.

Armed Forces Communications and Electronics Association. "The Russo-Georgian War 2008: The Role of Cyber Attacks in the Conflict." May 24, 2012. http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Anklam, Patti. *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World*. New York: Routledge, 2007.

Arquilla, John, and Douglas A. Borer. *Information Strategy and Warfare: A Guide to Theory and Practice*. New York: Routledge, 2007.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1993): 141–65. doi: 10.1080/01495939308402915.

———. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001.

Bakker, René M., Jörg Raab, and H. Brinton Milward. "A Preliminary Theory of Dark Network Resilience." *Journal of Policy Analysis and Management* 31, no. 1 (winter 2012): 33–62. doi: 10.1002/pam.20619.

Berger, J.M. "Social Media: An Evolving Front in Radicalization." U.S. Senate Committee on Homeland Security & Governmental Affairs. May 7, 2015. http://www.hsgac.senate.gov/hearings/jihad-20-social-media-in-the-next-evolution-of-terrorist-recruitment.

Boni, William C., and Gerald L. Kovacich. *Netspionage: The Global Threat to Information*. Boston: Butterworth-Heinemann, 2000.

Brachman, Jarret M. "High-Tech Terror: Al-Qaeda's Use of New Technology." *Fletcher Forum of World Affairs* 30, no. 2 (summer 2006): 149–64.

Brachman, Jarret, and James J.F. Forest. “Exploring the Role of Virtual Camps.” In *Denial of Sanctuary: Understanding Terrorist Safe Havens*, edited by Michael Innes, 124–48. Westport, CT: Praeger 2007.

Brachman, Jarret M., and William F. McCants. “Stealing Al Qaeda’s Playbook.” *Studies in Conflict & Terrorism* 29, no. 4 (July 2006): 309–21. doi: 10.1080/10576100600634605.

Brandom, Russell. “Cyberattacks Spiked as Russia Annexed Crimea.” *Verge*, May 29, 2014. http://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea.

Bugriy, Maksym. “The Crimean Operation: Russian Force and Tactics.” *Eurasia Daily Monitor* 11, no. 61, April 1, 2014. http://www.jamestown.org/regions/europe/single%20/?tx_ttnews%5Bpointer%5D=6&tx_ttnews%5Btt_news%5D=42164&tx_ttnews%5BbackPid%5D=51&cHash=fc393270652afcca3fe0563fcc63c5a0#.VVS9nZNyznd.

Bymer, Loren. “Virtual Reality Used to Train Soldiers in New Training Simulator.” *Army.mil*, August 1, 2012. http://www.army.mil/article/84453/.

Carroll, Ward. “Cyber War 2.0 — Russia v. Georgia.” *Defense Tech*, August 13, 2008. http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/.

Centola, Damon M. “Homophily, Networks, and Critical Mass: Solving the Start-up Problem in Large Group Collective Action.” *Rationality and Society* 25, no. 1 (February 2013): 3–40. doi: 10.1177/1043463112473734.

Christakis, Nicolas A., and James H. Fowler. *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives*. New York: Back Bay, 2009.

Clarion Project. “The Islamic State’s (ISIS, ISIL) Magazine.” September 2014. http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Tantor, 2014.

Coalson, Robert. “Top Russian General Lays Bare Putin’s Plan for Ukraine.” *World Post*, February 9, 2014. http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

Cox, Steven J. “Role of SOF in Paramilitary Operations.” Master’s thesis, Naval Postgraduate School, 1995. http://calhoun.nps.edu/handle/10945/31295.

Cruickshank, Paul, and Mohanad Hage Ali. "Abu Musab Al Suri: Architect of the New Al Qaeda." *Studies in Conflict & Terrorism* 30, no. 1 (January 2007): 1–14. doi: 10.1080/10576100601049928.

Cutler, Robert M. "Russia's Disinformation Campaign over South Ossetia." *Central Asia-Caucasus Institute Analyst* 10, no. 16 (August 2008): 6–8.

Darczewska, Jolanta. "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study" OSW Point of View, no. 42. Centre for Eastern Studies. May 2014.

Daugherty, William C. *Executive Secrets: Covert Action and the Presidency*. Lexington, KY: Univ. Press of Kentucky, 2006.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." *Security Dialogue* 43, no. 1 (February 2012): 3–24. doi: 10.1177/0967010611431079.

Denning, Dorothy E. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell, 170–86. Hershey, PA: Information Science Reference, 2011. doi: 10.4018/978-1-61692-805-6.

Department of the Army. *Army Special Operations Forces* [FM 3–05 (FM100-25)]. Washington, DC: Headquarters, Department of the Army, 2006.

———. *Army Special Operations Forces Unconventional Warfare* (FM 3–05.130). Washington, DC: Headquarters, Department of the Army, 2008.

———. *Special Forces: Unconventional Warfare* (TC 18–01). Washington, DC: Headquarters, Department of the Army, 2010. https://nsnbc.files.wordpress.com/2011/10/special-forces-uw-tc-18-01.pdf.

Duggan, Patrick Michael. "Strategic Development of Special Warfare in Cyberspace." *Joint Force Quarterly*, no. 79 (2015): 46–53.

Duncan, Kirk A. "Assessing the Use of Social Media in a Revolutionary Environment." Master's thesis, Naval Postgraduate School, 2013. http://calhoun.nps.edu/handle/10945/34660.

Eidman, Christopher R., and Gregory S. Green. "Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare." Master's thesis, Naval Postgraduate School, 2014. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA607604.

Everton, Sean F. “Tracking, Destabilizing and Disrupting Dark Networks with Social Networks Analysis” (Version 1.05). Naval Postgraduate School. 2008. http://calhoun.nps.edu/handle/10945/34415.

———. *Disrupting Dark Networks*. New York: Cambridge Univ. Press, 2012.

Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (2011): 23–40. doi: 10.1080/00396338.2011.555586.

Franke, Ulrik. “War by Non-Military Means: Understanding Russian Information Warfare.” Swedish Defence Research Agency. 2015. http://www.foi.se/ReportFiles/foir_4065.pdf.

Friedman, George. “The Russo-Georgian War and the Balance of Power.” *Stratfor*, August 12, 2008. http://blog.cafewall.com/wp-content/uploads/2008/09/rus-v-geo-analysis.pdf.

Gerasimov, Valery. “The New Generation Warfare.” *VPK News*, March 27, 2013. http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

Ghannam, Jeffrey. “Social Media in the Arab World: Leading up to the Uprisings of 2011.” Center for International Media Assistance. February 2011. http://www.databank.com.lb/docs/Social%20Media%20in%20the%20Arab%20World%20Leading%20up%20to%20the%20Uprisings%20of%202011.pdf.

Giles, Keir. “‘Information Troops’-A Russian Cyber Command.” Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, June 7–10, 2011. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5954699.

Godson, Roy. *Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence*. New Brunswick, NJ: Transaction, 1995.

Goel, Sanjay. “Cyberwarfare: Connecting the Dots in Cyber Intelligence.” *Communications of the ACM* 54, no. 8 (August 2011): 132–40. doi: 10.1145/1978542.1978569.

Goldman, Adam. “Two Men in Boston Charged with Planning to Aid Islamic State.” *Washington Post*, June 12, 2015. https://www.washingtonpost.com/world/national-security/two-men-in-boston-charged-with-planning-to-aid-the-islamic-state/2015/06/12/c8cd2c3a-1110-11e5-9726-49d6fa26a8c6_story.html.

Gordon, Michael R. “Russia Displays a New Military Prowess in Ukraine’s East.” *New York Times*, April 21, 2014. http://www.nytimes.com/2014/04/22/world/europe/new-prowess-for-russians.html?_r=0.

Gould, Roger V. “Collective Action and Network Structure.” *American Sociological Review* 58, no. 2 (April 1993): 182–96. doi: 10.2307/2095965.

Granovetter, Mark S. “The Strength of Weak Ties.” *American Journal of Sociology* 78, no. 6 (May 1973): 1360–80.

Harris, Shane. “Hack Attack: Russia’s First Targets in Ukraine: Its Cell Phones and Internet Lines.” *Foreign Policy*, March 3, 2014. http://foreignpolicy.com/2014/03/03/hack-attack/.

Hart, Kim. “Longtime Battle Lines Are Recast in Russia and Georgia’s Cyberwar.” *Washington Post*, August 14, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html.

Helfstein, Scott. “Edges of Radicalization: Ideas, Individuals and Networks in Violent Extremism.” U.S. Military Academy, Combating Terrorism Center. February 2012. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA556711.

Hilsman, Roger. *American Guerrilla: My War behind Japanese Lines*. Nebraska: Potomac Books, 1990.

Hollis, David. “Cyber War Case Study: Georgia 2008.” *Small Wars Journal* 7, no. 1 (January 2011).

Irwin, Will. *The Jedburghs: The Secret History of the Allied Special Forces, France 1944*. New York: Public Affairs, 2009.

Janos, Andrew C. “Unconventional Warfare: Framework and Analysis.” *World Politics* 15, no. 4 (July 1963): 636–46. doi:10.2307/2009460.

Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms* (JP 1–02). Washington, DC: Joint Chiefs of Staff, 2010. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf: 263.

———. *Cyberspace Operations* [JP 3–12 (R)]. Washington, DC: Joint Chiefs of Staff, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

———. *Special Operations* (JP 3–05). Washington, DC: Joint Chiefs of Staff, 2014. http://dtic.mil/doctrine/new_pubs/jp3_05.pdf.

Joint Staff, J-7. *Planner’s Handbook for Operational Design*. Suffolk, VA: Joint Staff, 2011. http://www.au.af.mil/au/awc/awcgate/dod/opdesign_hbk.pdf.

Jones, Derek. “Ending the Debate: Unconventional Warfare, Foreign Internal Defense, and Why Words Matter.” Master’s thesis, U.S. Army Command and General Staff College, 2006. http://ftp.fas.org/man/eprint/jones.pdf.

Karagiannis, Emmanuel. "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals." *Contemporary Security Policy* 35, no. 3 (September 2014): 400–20. doi: 10.1080/13523260.2014.963965.

Karatzogianni, Athina. "Blame it on the Russians: Tracking the Portrayal of Russians During Cyber conflict Incidents." *Digital Icons: Studies in Russian, Eurasian and Central European New Media* 4 (2010): 128–50.

Kirk, Jeremy. "Georgia Cyberattacks Linked to Russian Organized Crime," *Computerworld*, August 17, 2009. http://www.computerworld.com/article/2527019/government-it/georgia-cyberattacks-linked-to-russian-organized-crime.html.

Korns, Stephen W., and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* 38, no. 4 (winter 2008–9): 60–76.

Krebs, Brian. "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks." *Washington Post*, October 16, 2008. http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

Kriesi, Hanspeter. "The Organizational Structure of New Social Movements in a Political Context." In *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, edited by Doug McAdam, John D. McCarthy, and Mayer N. Zald, 152–204. Cambridge, U.K.: Cambridge Univ. Press, 1996.

Lacey, Jim. *A Terrorist's Call to Global Jihad: Deciphering Abu Musab Al-Suri's Islamic Jihad Manifesto*. Annapolis, MD: Naval Institute, 2008.

Lazar, Marian. "Russian Cyber Campaign against Georgia." In *The Complex and Dynamic Nature of the Security Environment*, 500–6. Bucharest, Romania: National Defense Univ., 2012.

Lebow, Richard Ned, and Thomas Risse-Kappen. *International Relations Theory and the End of the Cold War*. New York: Columbia Univ. Press, 1996. http://nuesaui2014.com/ebooks/political%20science/International%20relation%20Theory.pdf.

Lee, Doowan. "A Social Movement Approach to Unconventional Warfare." *Special Warfare* 26, no. 3 (September 2013) 27–32.

Lee, Doowan, and Glenn W. Johnson. "Revisiting the Social Movement Approach to Unconventional Warfare." *Small Wars Journal*, December 1, 2014. http://smallwarsjournal.com/jrnl/art/revisiting-the-social-movement-approach-to-unconventional-warfare.

Lerner, Melissa Y. "Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt." *Journal of Muslim Minority Affairs* 30, no. 4 (December 2010): 555–74. doi: 10.1080/13602004.2010.533453.

Lewis, James A. "Assessing the Risks of Cyber Terrorism: Cyber War and Other Cyber Threats." Center for Strategic and International Studies. 2002.

Leyden, John. "Bear Prints Found on Georgian Cyber-attacks." *Register*, August 14, 2008. http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/.

Lia, Brynjar. *Architect of Global Jihad: The Life of Al-Qaida Strategist Abu Mus'ab Al-Suri*. London: Hurst, 2014.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

Liles, Samuel. "Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency." Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, June 7–10, 2011. https://ccdcoe.org/publications/2010proceedings/Liles%20-%20Cyber%20warfare%20%20As%20a%20form%20of%20low-intensity%20conflict%20and%20insurgency.pdf.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (2010): 97–108.

Malik, Shiv, Mark Tran, Kim Willsher, Anne Penketh, and Alexandra Topping. "Paris Supermarket Attacker Claims Allegiance to Islamic State in Video." *Guardian*, January 11, 2015. http://www.theguardian.com/world/2015/jan/11/paris-supermarket-attacker-islamic-state-video-isis-amedy-coulibaly.

Markoff, John. "Before the Gunfire, Cyberattacks." *New York Times*, August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&.

Marwell, Gerald, Pamela E. Oliver, and Ralph Prahl. "Social Networks and Collective Action: A Theory of the Critical Mass. III." *American Journal of Sociology* 94, no. 3 (1988): 502–34.

McAdam, Doug. "Social Movements and Conflicts." Naval Postgraduate School. 2010.

McAdam, Doug, John D. McCarthy, and Mayer N. Zald, eds. *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*. Cambridge: Cambridge Univ. Press, 1996.

McAdam, Doug, John D. McCarthy, and Mayer N. Zald. "Introduction: Opportunities, Mobilizing Structures, and Framing Processes - toward a Synthetic, Comparative Perspective on Social Movements." In *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, edited by Doug McAdam, John D. McCarthy, and Mayer N. Zald, 1–20. Cambridge: Cambridge Univ. Press, 1996.

McBride, Michael, and David Hewitt. "The Enemy You Can't See: An Investigation of the Disruption of Dark Networks." *Journal of Economic Behavior & Organization* 93 (September 2013): 32–50. doi: 10.1016/j.jebo.2013.07.004.

McCarthy, John D. "Constraints and Opportunities in Adopting, Adapting, and Inventing." In *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, edited by Doug McAdam, John D. McCarthy, and Mayer N. Zald, 142–51. Cambridge: Cambridge Univ. Press, 1996.

Menn, Joseph. "Expert: Cyber-attacks on Georgia websites Tied to Mob, Russian Government," *Los Angeles Times*, August 13, 2008, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

Morris, Aldon. "Reflections on Social Movement Theory: Criticisms and Proposals." *Contemporary Sociology* 29, no. 3 (May 2000): 445–54. doi: 10.2307/2653931.

Morris, Aldon D., and Carol McClurg Mueller. *Frontiers in Social Movement Theory*. New Haven, CT: Yale Univ. Press, 1992.

Mosendz, Polly. "Report: Shooters at Garland, Texas Muhammad Cartoon Event Linked to ISIS." *Newsweek*, May 4, 2015. http://www.newsweek.com/report-shooters-garland-texas-muhammad-cartoon-event-linked-isis-328267.

Newton, Richard D., Travis L. Homiak, Kelly H. Smith, Isaac J. Peltier, and D. Jonathan White. *Contemporary Security Challenges: Irregular Warfare and Indirect Approaches* (Hurlburt Field, FL: Joint Special Operations Univ. Press, 2009.

Nye, Joseph S., Jr. "Cyber Power." Harvard Kennedy School, Belfer Center for Science and International Affairs. May 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626

Oliver, Pamela E. "Formal Models of Collective Action." *Annual Review of Sociology* 19 (1993): 271–300.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge: Harvard Univ. Press, 2009.

Opp, Karl-Dieter. *Theories of Political Protest and Social Movements: A Multidisciplinary Introduction, Critique, and Synthesis*. London: Routledge, 2009.

Ostrom, Elinor. “A Behavioral Approach to the Rational Choice Theory of Collective Action: Presidential Address, American Political Science Association, 1997.” *American Political Science Review* 92, no. 1 (March 1998): 1–22. doi: 10.2307/2585925.

———. “Analyzing Collective Action.” *Agricultural Economics* 41, no. s1 (November 2010): 155–66. doi: 10.1111/j.1574-0862.2010.00497.x.

———. “Collective Action and the Evolution of Social Norms.” *Journal of Natural Resources Policy Research* 6, no. 4 (2014): 235–52. doi: 10.1080/19390459.2014.935173.

Paddock, Alfred H., Jr. U.S. *Army Special Warfare, Its Origins: Psychological and Unconventional Warfare, 1941–1952*. Honolulu: Univ. Press of the Pacific, 2002. http://books.google.com/books?hl=en&lr=&id=3pWi0xfw6q0C&oi=fnd&pg=PR9&dq=%22Coordinator+of+Information%22+%22of+OSS%22+%22Joint+Subsidiary+Plans+Division%22+%22and+Unconventional+Warfare%22+%22Office+of+Policy+Coordination%22+%22Propaganda+Branch,+G-2%22+%22Assistance+to%22+%22Toward+Unconventional+Warfare%22+%22and+Psychological+Warfare+in+Korea%22+&ots=0G4XrxhtgR&sig=IXbLGndXBHKQGUScb8XvCOU_uDY.

Paganini, Pierluigi. “Crimea—The Russian Cyber Strategy to Hit Ukraine.” *InfoSec Institute*, March 11, 2014. http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.

Peers, William R., and Dean Brelis. *Behind the Burma Road: The Story of America’s Most Successful Guerrilla Force*. Boston: Little Brown, 1963.

Pellerin, Cheryl. “Cybercom Chief: Cyber Threats Blur Roles, Relationships.” *Department of Defense News*, March 6, 2015. http://www.defense.gov/News-Article-View/Article/604225.

Petit, Brian. “Social Media and UW.” *Special Warfare Magazine* 25, no. 2 (2012): 21–28. http://www.soc.mil/swcs/swmag/archive/SW2502/SW2502SocialMediaAndUW.html.

Prell, Christina. *Social Network Analysis: History, Theory and Methodology*. London: SAGE, 2012.

Reuter, Christoph. “The Terror Strategist: Secret Files Reveal the Structure of Islamic State.” *Spiegel Online International*, April 18, 2015. http://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html.

Roberts, Nancy, and Sean F. Everton. “Strategies for Combating Dark Networks.” *Journal of Social Structure* 12, no. 2 (2011): 1–32. http://calhoun.nps.edu/public/handle/10945/41260.

Sacquety, Troy James. “The Organizational Evolution of OSS Detachment 101 in Burma, 1942–1945.” Doctoral dissertation, Texas A&M Univ., 2008. http://repository.tamu.edu/bitstream/handle/1969.1/ETD-TAMU-3280/SACQUETY-DISSERTATION.pdf?sequence=1&isAllowed=y.

Salanova, Regina. “Social Media and Political Change: The Case of the 2011 Revolutions in Tunisia and Egypt” Working Paper no. 2012/7. International Catalan Institute for Peace. December 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2206293.

Seldin, Jeff. “Report: Kremlin Was Eying Ukraine Prior to Yanukovych Ouster.” *Voice of America*, February 24, 2015. http://www.voanews.com/content/russia-ukraine-novaya-gazeta-strategic-document/2657107.html.

Shakarian, Paolo. “The 2008 Russian Cyber Campaign against Georgia.” *Military Review* 91, no. 6 (November-December 2011): 63–68.

Shuster, Brian. “Could Virtual Reality Revitalize the Economy?” *Wired*, October 2014. http://www.wired.com/2014/10/virtual-reality-economy/.

Sindelar, Daisy. “Inside Russia’s Disinformation Campaign.” *Atlantic*, August 12, 2014. http://www.defenseone.com/technology/2014/08/inside-russias-disinformation-campaign/91286/.

Socor, Vladimir. “Crimea: From Russian Putsch to Military Invasion and Possible Occupation.” *Eurasia Daily Monitor* 11, no. 41, March 4, 2014. http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=42036&cHash=d022abf71c498ee019b60572d6593ea1#.VVTAUZNyznd.

Special Warfare Center and Schools. *A Leader’s Handbook to Unconventional Warfare* (SWCS PUB 09–1). Fort Bragg, NC: Special Warfare Center and School, 2009.

Stent, Angela, and Lilia Shevtsova. “America, Russia and Europe: A Realignment?” *Survival* 44, no. 4 (2002): 121–34. doi: 10.1080/00396330212331343532.

Stern, Jessica, and J.M. Berger. *ISIS: The State of Terror*. New York: HarperCollins, 2015.

Synovitz, Ron. “Russian Forces in Crimea: Who Are They and Where Did They Come From?” *Radio Free Europe/Radio Liberty*, March 4, 2014. http://www.rferl.org/content/russian-forces-in-crimea--who-are-they-and-where-did-they-come-from/25285238.html.

Tarrow, Sidney. “States and Opportunities: The Political Structuring of Social Movements.” In *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, edited by Doug McAdam, John D. McCarthy, and Mayer N. Zald, 41–61. Cambridge Univ. Press, 1996.

Thomas, Timothy L. “The Bear Went through the Mountain: Russia Appraises its Five-Day War in South Ossetia.” *Journal of Slavic Military Studies* 22, no. 1 (2009): 31–67. doi: 10.1080/13518040802695241.

Tierney, John J., Jr. *Chasing Ghosts: Unconventional Warfare in American History* Washington, DC: Potomac, 2006.

U.S. Army Cyber Command. “USCYBERCOM.” Accessed October 25, 2015. http://www.arcyber.army.mil/org-uscc.html.

U.S. Army Special Operations Command. “ARSOF 2022.” *Special Warfare Magazine* 26, no. 2 (April-June 2013).

———. “Counter-Unconventional Warfare” (White Paper). September 26, 2014.

———. “ARSOF 2022 Part 2: Changing the Institution.” *Special Warfare Magazine* 27, no. 3 (September 2014).

U.S. Department of State. Bureau of International Information Programs. “U.S. Offers $5 Million Reward for Information about Terrorist.” *GlobalSecurity.org*, November 18, 2004. http://www.globalsecurity.org/security/library/news/2004/11/sec-041118-usia01.htm.

United States Special Operations Command. *Organization and Functions: Terms of Reference--Roles, Missions, and Functions of Component Commands*. USSOCOM Directive 10–1. MacDill Air Force Base, FL: United States Special Operations Command, 2009. https://jsou.blackboard.com/bbcswebdav/library/Library%20Content/JSOU%20References/JSOU-ISOF/ISOF%20References/USSOCOM%20Directive%2010-1%2015%20Dec%2009.pdf.

Washington Post. “Timeline: Key Events in Ukraine’s Ongoing Crisis.” May 12, 2014. http://www.washingtonpost.com/world/europe/timeline-key-events-in-ukraines-ongoing-crisis/2014/05/07/a15b84e6-d604-11e3-8a78-8fe50322a72c_story.html.

Weimann, Gabriel. “www.terror.net: How Modern Terrorism Uses the Internet” Special Report 116. United States Institute of Peace. March 2004. http://books.google.com/books?hl=en&lr=&id=a_cugt6quTYC&oi=fnd&pg=PA2&dq=%22of+the+World+Wide%22+%22Terrorism+on+the+Internet+is+a+very+dynamic+phenomenon:+websites+suddenly%22+%22uses+made+of+the+Internet.+Those+uses+are+numerous+and,+from+the%22+&ots=JiC6c1Iry2&sig=taVdPF__glV5ba6ru6MjQBSFNZ4.

Weir, Fred. “Russia Debuts New, Sleek Force in Crimea, Rattling NATO.” *Christian Science Monitor*, April 3, 2014. http://www.csmonitor.com/World/Europe/2014/0403/Russia-debuts-new-sleek-force-in-Crimea-rattling-NATO.

Weiss, Michael. “Russia Stages a Coup in Crimea.” *Daily Beast*, March 1, 2014. http://www.thedailybeast.com/articles/2014/03/01/so-russia-invaded-crimea.html.

Wenner, Randall D. “Detachment 101 in the CBI: An Unconventional Warfare Paradigm for Contemporary Special Operations.” Master’s thesis, U.S. Army Command and General Staff College, 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA523185.

Woehrel, Steven. *Ukraine: Current Issues and U.S. Policy* (CRS Report No. RL33460). Washington, DC: Congressional Research Service, 2011. http://fpc.state.gov/documents/organization/164374.pdf.

Zabel, Sarah E. “The Military Strategy of Global Jihad.” Strategic Studies Institute. October 2007. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB809.pdf.

Zackie, M. W. “An Analysis of Abu Mus’ab Al-Suri’s ‘Call to Global Islamic Resistance.’” *Journal of Strategic Security* 6, no. 1 (March 2013): 1–18. doi: 10.5038/1944-0472.6.1.1.

Zafar, Shaarik H. “Western Foreign Fighters in Syria: Implications for U.S. CVE Efforts.” *Washington Institute for Near East Policy*, March 14, 2014. http://www.washingtoninstitute.org/policy-analysis/view/western-foreign-fighters-in-syria-implications-for-u.s.-cve-efforts.

Zald, Mayer N. “Culture, Ideology, and Strategic Framing.” In *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, edited by Doug McAdam, John D. McCarthy, and Mayer N. Zald, 261–74. Cambridge Univ. Press, 1996.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California